Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 5555362, 10 pages
https://doi.org/10.1155/2021/5555362

*Review Article*

# Searchable Encryption with Access Control in Industrial Internet of Things (IIoT)

**Jawhara Bader**[1,2] **and Anna Lito Michala**[1]

[1]*School of Computing Science, University of Glasgow, Glasgow G12 8RZ, UK*
[2]*Department of Computer Science, Faculty of Computers and Information Technology, University of Tabuk, Tabuk, Saudi Arabia*

Correspondence should be addressed to Jawhara Bader; j.alamri.1@research.gla.ac.uk

Received 4 February 2021; Revised 31 March 2021; Accepted 29 April 2021; Published 17 May 2021

Academic Editor: Mohammad R. Khosravi



The technological advancements in the Internet of Things (IoT) and related technologies lead to revolutionary advancements in many sectors. One of these sectors, is the industrial sector red that leverages IoT technologies forming the Industrial Internet of Things (IIoT). IIoT has the potential to enhance the manufacturing process by improving the quality, trace-ability, and integrity of the industrial processes. The enhancement of the manufacturing process is achieved by deploying IoT devices (sensors) across the manufacturing facilities; therefore, monitoring systems are required to collect (from multiple locations) and analyse the data, most likely in the cloud. As a result, IIoT monitoring systems should be secure, preserve the privacy, and provide real-time responses for critical decision-making. In this review, we identified a gap in the state-of-the-art of secure IIoT and propose a set of criteria for secure and privacy preserving IIoT systems to enhance efficiency and deliver better IIoT applications.

## 1. Introduction

The Internet of Things (IoT) has gained enormous popularity in the last decade, which consists of interconnected devices such as mobile phones, computers, sensors, and many more. These devices helped to develop and improve many sectors, such as Smart Cities, Smart Homes, and Healthcare [1]. The significant improvement added to these sectors encouraged the industrial sector to introduce IoT into the manufacturing paradigm. As a result, this led to a new industrial revolution: Industry 4.0. A new term Industrial Internet of Things (IIoT) has been used to collectively refer to proposed IoT solutions in this space [2].

The applications of IIoT can be classified into four categories (Figure 1). The first class includes production flow, quality control, and energy consumption. This class is aimed at improving production processes. The second class is operation-oriented management, which includes supply chain and enterprise decision management. The third class focuses on the allocation and collaboration of resources. This class includes collaborative manufacturing and customization technology. Finally, the last class mainly focuses on product life cycle management. Additionally, it focuses on service optimization, such as remote maintenance and product traceability [2].

The growing population has led to an increasing demand for products, which has saturated the manufacturing industry and even more so in the recent COVID crisis. As a result, the manufacturing segment is expected to have the highest and fastest-growing market segment by end-user at a compound annual growth rate (CAGR) of 27.94%. To meet the growing demand, an efficient manufacturing system has become mandatory. This demand can only be achieved by the integration of the latest technologies, such as IoT within the manufacturing process [3]. However, the stringent regulatory requirements (COMAH, IEC, and SIL) for safety must be satisfied for this shift to become usable in real-world applications.

To demonstrate the relevance of IIoT and its ability to meet regulatory requirements, we present two examples of manufacturers currently using IIoT schemes [4]. The first one is Airbus, the European aircraft manufacturer. Airbus currently integrates IoT technologies into its products and its workers' tools in the manufacturing process. Also, Airbus

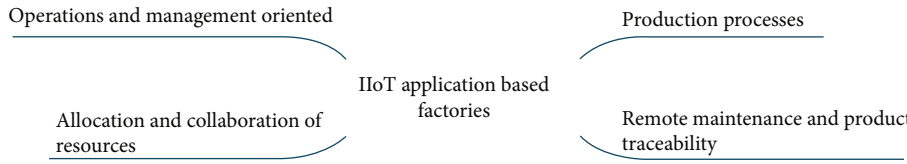


Figure 1: IIoT application-based factories.

is harnessing IoT technologies to clear a backlog of orders and boost revenues. It is clear that IoT is transforming the aviation industry by enabling a more seamless passenger journey, increasing operational efficiency, and driving a new age of "connected aviation." The second example is the global tech firm Client Global Insights (CGI). CGI has teamed up with Microsoft to deliver a predictive maintenance solution for elevators by leveraging IoT. CGI claims that it has developed a solution which securely connects thousands of sensors and systems within elevators and monitors everything from motor temperature to shaft alignment. The data are collected and processed on the cloud using Microsoft's cloud-based Azure Intelligent Systems Service. These elevators enable technicians to use real-time IIoT data to spot defects and repair them before a breakdown occurs.

Thus IIoT, such as monitoring systems, help industries improve their resources and meet their clients' needs while ensuring high-quality production. IIoT achieves this by providing ubiquitous connectivity, efficient data analytics tools, better decision support systems, and applications [5, 6]. As IIoT applications deal with complicated processes, these applications have a critical impact on several parties. For example, a failure in an IIoT application may put the employees' lives in the factory at severe risk. Similarly, the business resources may be at risk which has cost implications [7]. Therefore, the accuracy, precision, and risk impact of application-failure metrics of IIoT applications should be higher than in IoT applications. Moreover, IIoT applications must fulfil the stringent requirements of real-time processing and feedback, time synchronisation, and regular communication [8].

The three essential components of security are confidentiality, integrity, and availability, which are known as the CIA triangle. Confidentiality ensures that only authorised users can read the data of a system. Integrity ensures that no changes are made to the data, and availability means that all services and data are available [9]. Availability and integrity of data are considered more essential than confidentiality for industrial environments. This, however, does not diminish the need for confidentiality. With the internet-connected systems of IIoT, all three aspects should be brought up to an acceptable level. Thus, in the development of new IIoT and Industry 4.0 systems that leverage the existing network and cloud infrastructure, confidentiality and integrity should be weighed equally to availability [10].

IIoT applications, such as monitoring systems in smart factories, work by collecting data from multiple locations and analysing the data on the cloud. However, collecting and processing data on the cloud compromise the data privacy and security, leading to sensitive information leakage [11, 12]. Data-at-rest must be securely stored and processed on the cloud without compromising its security and privacy [11, 13]. This goal is challenging as it requires processing the encrypted data (not the plaintext) on the cloud. Moreover, some IIoT applications require access control (AC) policies to allow specific users, such as a manager or a third-party contractor to access and query the data. This AC requirements adds a more significant challenge [14, 15]. To highlight the need for data confidentiality and integrity in IIoT applications, the authors in [16] demonstrated how collecting air-quality-related data on unsecure servers can misinform the public or mislead policymakers. The authors showed that any modification to the sensors' data can lead to false-negative emergency alerts or wrong decisions. An example of wrong decisions is triggering the evacuation alarm or stopping a production line. Therefore, it is crucial for IIoT applications to secure the collected data. This can be achieved by encrypting the collected data during transmission and at-rest [17].

The degree of severity in relation to violating privacy on the IIoT differs from that of the IoT. In IoT, unauthorised access may lead to privacy problems such as data theft. On the other hand, violating privacy on IIoT may lead to a disastrous decision that can cause the entire system to fail [7]. IoT and IIoT may share similar security threats. Yet, there is a substantial difference between the degree of severity in the event of a security breach in both IoT and IIoT [18]. In other words, authenticating an illegitimate device may cause a normal IoT system to experience some problems, such as privacy invasion. On the other hand, a similar scenario in an IIoT system could cause serious consequences. For example, disrupting the network or forcing the network to take hazardous actions. Thus, IIoT requires a higher level of security. To do so, there are several factors to consider, such as the applications' requirements, the type of IIoT devices, and a recovery technique in the case of cybersecurity attack [19].

In addition to the previous security and privacy requirements, factories need to share the data with other parties, such as insurance or/and consulting companies, customers, and/or employees. To control and manage data access, IIoT systems must deploy AC mechanisms on the encrypted data on the cloud [20].

Several recent studies have addressed the security and privacy issues for IIoT, from different perspectives. For example, the authors of [17] categorised the security challenges for both IoT and IIoT. The authors also specified whether these challenges are applicable to IoT or IIoT or both. On the other hand, the study demonstrates the security challenges in the IIoT and stresses the need to design practical solutions. Also, the study shows that various IIoT scenarios require application-specific designs. However, solutions to the challenge of appropriate designs are not suggested by the authors.

In [21], the authors analysed the security challenges of IIoT and provided a comparative analysis of the available solutions. This study set out to identify some open research problems related to system integration, communication, energy factor, preventive and detective measures, authorisation, and architecture of IIoT. However, the study does not suggest feasible and practical solutions. Similarity, Tange et al. [10] provide a systematic literature review of IIoT security requirements. The authors demonstrate how fog computing can address these requirements. Additionally, the authors identified some research opportunity to use secure fog computing for IIoT.

uilding on existing findings from [10, 17, 21], in this article, we examined the practical considerations of embedding security and privacy solutions to IIoT system architectures moving away from the cloud paradigm to minimise exposure to threats. Thus, we focus on combining searchable encryption and access control methods in a cloud-Edge architecture to assess their suitability and efficiency from the privacy, security, and response time perspectives.

## 2. Objectives

In the context of IIoT, privacy refers to protecting the confidentiality of the IIoT device and its collected readings (data). For example, exposing the sensor's location is considered a security and safety threat. The lack of privacy preservation causes security threats, such as in the case of utility monitoring, which will affect the network's process [19]. To address the aforementioned requirements for security and privacy in IIoT monitoring systems, we must consider the following challenges:

(1) *The Limited Resources in IIoT Devices, such as Low Computational Power, Low Power Consumption, and Low Storage*. Therefore, deploying and running encryption algorithms on these devices may add significant performance overhead.

(2) *The Adaptation of Searchable Encryption (SE)*. Searching the encrypted data on the cloud requires adapting and enhancing searchable encryption (SE) algorithms to work on both the cloud and IIoT devices.

(3) *The Critical Real-Time Requirement for IIoT Systems*. IIoT monitoring systems should fulfill the critical real-time requirement, which significantly affects the decision-making process. Thus, each component in the system should be optimised to reduce the overall execution time.

The security aspects and requirements in IIoT can be identified as follows [22]:

(i) *Impact of Attack*. A successful attack on an IIoT system has a high impact due to the critical nature of this industry.

(ii) *Secure Communication*. It is important to maintain a secure connection between IIoT parties. Unsecure communication channels can expose sensitive information.

(iii) *Authentication and Authorisation*. IIoT requires authentication and authorisation for all connected devices. This includes but not limited to, sensors, internal users, and external users.

(iv) *Accountability*. It is important to keep track of all actions and incidents in an IIoT system to identify and recover from any possible incidents. According to [23], the main security concerns are authentication and access control. The reason is that users with improper access rights can severely affect these systems.

In this paper, we aimed to examine the state-of-the-art in security and privacy of IIoT application systems and focus on the combination between searchable encryption and access control methods applied on Edge computing to assess their suitability and efficiently from a privacy, security, and response time perspective. Hence, the present article is aimed at fostering scientific discussion regarding IIoT from the privacy and security perspective under constraints by revealing the current state of research as well as identifying areas to be addressed by future research efforts. By doing so, the following research questions are pursued:

(i) *RQ1*. Which research areas and methods have addressed the security, privacy, and efficiently performance of IIoT and to what extend so far?

(ii) *RQ2*. Which research areas or methods can be proposed to further security and privacy improvement in the future of smart factories?

To answer the abovementioned questions, a systematic review of relevant literature is applied as presented in Section 3. The results of the literature search are presented in Section 4 where we taxonomise relevant research. A discussion of the findings along with open challenges and suggested areas of further research is presented in Section 5 with conclusions presented in Section 6.

## 3. Methods

We selected a list of publications related to IIoT systems to be included in the comparative analysis. The databases and sources used in this systematic review include (1) IEEE, (2) Springer, (3) websites of smart factories found through a generic Google search, and (4) Google Scholar (including ResearchGate).

We focused on several topics, including security in IIoT, enhanced searchable encryption algorithms, and a combination between searchable encryption, and access control methods. The search keywords alongside the number of results are presented in Table 1.

As the above combination of data sources and keywords returned a vast amount of results, we selected the following inclusion criteria to identify the most relevant sources: (1) language: English, (2) date range: within the past five years (2017-2020), (3) the article presents a review or a survey

Table 1: Results of the literature search.

| Topic | Online library | Number of results |
|---|---|---|
| Industrial Internet of Things applications | IEEE | 2,845 |
| | Springer | 44,937 |
| | Google search | 53,000 |
| | Google Scholar | 100,000 |
| Searchable encryption for IIoT | IEEE | 9 |
| | Springer | 8 |
| | Google search | 124 |
| | Google Scholar | 120 |
| Access control for IIoT | IEEE | 101 |
| | Springer | 898 |
| | Google search | 5,600 |
| | Google Scholar | 5,000 |
| Privacy preserving for IIoT applications | IEEE | 19 |
| | Springer | 114 |
| | Google search | 1,000 |
| | Google Scholar | 1,110 |
| Edge computing in IIoT application | IEEE | 89 |
| | Springer | 483 |
| | Google search | 3,150 |
| | Google Scholar | 3,000 |
| Requirements of IIoT | IEEE | 238 |
| | Springer | 1,057 |
| | Google search | 5,000 |
| | Google Scholar | 4,580 |
| Searchable encryption with access control | IEEE | 105 |
| | Springer | 1,168 |
| | Google search | 2,300 |
| | Google Scholar | 10,000 |
| Monitoring system using IIoT | IEEE | 125 |
| | Springer | 967 |
| | Google search | 5,200 |
| | Google Scholar | 15,100 |
| Security of IIoT applications | IEEE | 197 |
| | Springer | 853 |
| | Google search | 4,600 |
| | Google Scholar | 5,030 |

related to IIoT, and (4) relevance: searchable encryption with access control for Edge-based IIoT application is necessary. The exclusion criteria are as follows: (1) nonrelated to the relevance inclusion criteria, (2) implicitly related the relevance inclusion criteria, (3) duplicate articles that appear multiple times in one or more databases, and (4) nonresearch article.

Those four exclusion criteria and four inclusion criteria as illustrated above improved the objectivity of this review paper. A filtering process was carried out to exclude those articles that fulfill the exclusion criteria. The remaining articles were classified according to the four inclusion criteria, and data of interest was collected.

## 4. Results

The literature search returned a total of 268,507 results. Overall, we read 235 sources, as we excluded the majority by reading the abstracts. A total of 54 sources remained for analysis and were taxonomised as seen in Figure 2.

*4.1. State-of-the-Art in IIoT with Embedded Security Mechanisms.* IIoT systems can benefit from the massive amount of collected data to generate a useful approach. This approach can improve the performance of the system and minimise unplanned downtime [24]. IIoT systems utilise cloud servers to store and process the generated massive data [24]. However, the data need time to be transferred to centralized data centres, which degrades the IIoT system efficiency. This implies that processing data on an Edge server could help the IIoT system meet real-time requirements and reduce the decision-making latency [25]. The survey presented in [17] identified two constraints when protecting data confidentiality in IIoT systems through data encryption. One of these constraints is related to the limited resources of IIoT devices.

Gebremichael et al. [19] describe the privacy challenges in IIoT based on the levels of the architecture as follows: device, platform, and application layers. The solutions provide access control methods, authentication mechanisms, data encryption, and secure channels to ensure the privacy at the device layer, for example, protecting Edge nodes against a fake node insertion attack. They also describe several points that developers need to consider when designing privacy solutions for the IIoT. These points can be described as follows:

(i) Cryptographic mechanisms are generally employed to enforce privacy policies. The challenge is to design a lightweight privacy-enhancing cryptosystem suitable for IIoT devices. These IIoT devices have limited resources. Thus, it is crucial to prevent heavy computations to meet the IIoT real-time requirement

(ii) Further research is needed to provide lightweight cryptosystem solutions with anonymised data methods. Also, advanced data analytics tools to process the collected data

(iii) Reducing the amount of data collected by Edge devices to the minimum data points that are required for system operations while continuing to provide anonymisation techniques on user data

(iv) Illustrating data access policies and implementing appropriate access control methods that are capable of identifying authorised users that have access rights to Edge node data

Several solutions can protect IIoT systems' privacy, such as encryption, access control, processing data on the Edge, and anonymisation. Privacy in IIoT systems is challenging as these systems usually store and process data in third-party cloud services.

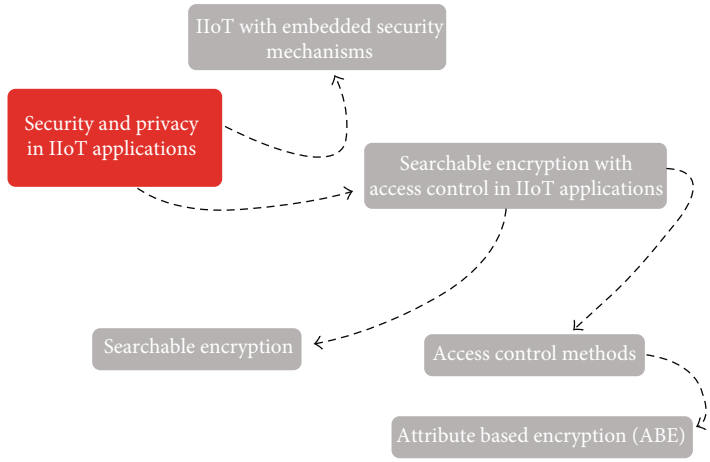


Figure 2: Literature article categories.

Yu et al. state that the data generated by IoT devices has increased dramatically. At the same time, Cisco predicted that the volume of data generated by IoT devices would reach 500 ZB by 2019 [26]. However, massive data need time to be transferred directly to the cloud for processing, which adds computation overhead. This computation overhead increases the latency, bandwidth, and may even lead to the unavailability of IIoT applications [2]. To address this issue, the concept of Edge/fog computing has been defined, and data can now be processed much closer to the source. This is because some cloud services are brought to the Edge of the network. In this context, fog computing differs from Edge computing in that it uses the interconnection between endpoints. Edge computing, on the other hand, focuses on isolated endpoints [26]. This implies that processing data on the Edge server helps the IIoT system to meet the real-time requirement and reduce decision-making latency, especially for delay-sensitive applications [2]. Edge computing is applied to manufacturing based on IoT to meet these requirements [27].

Many researchers introduced improvements to searchable encryption algorithms that would make them lightweight for IIoT, such as [28]. Yet, this method is not tested for its applicability in industrial plants. Wazid et al. [29] review the access control in IIoT such as a monitoring system of an industrial plant. They state that authentication is the most important security requirement in cloud-based IIoT while this requirement is still needed to improve the proposed solution.

The following subsections will discuss data analtyics, searchable encryption, and access control state-of-the-art methods that have the potential to address the challenges identified in this subsection.

*4.2. Edge Data Analytics for IIoT Applications.* Data analytics is the most important step in the monitoring system's life cycle. IoT data analytics improves fault detection, disaster forecasting, service, and smart decision-making [30]. Moreover, they help the smart factory extract the knowledge from raw data with the support of IIoT applications, for example, to better understand technological enabler behaviour or to relate issues derived from combined and statistical data processing [31]. The usage of feature extraction methods provides more accurate data analysis results. Besides, meeting the real-time requirement for IIoT manufacturing applications, for instance, a robust incremental feature extraction method based on PCA (Principal Component Analysis) is proposed to meet the real-time requirement [30]. Extracting data features from the data by applying such techniques allows Edge servers to take smart decisions for delay-sensitive applications [27]. Applying Edge analytics directly reduces the volume of data to be transmitted to the cloud. This, in turn, reduces the information that must be encrypted, which makes the encryption overhead minor. However, this reduction introduces other challenges in terms of accuracy and traceability, especially in regard to the route cause fault finding capabilities. Thus, appropriate Edge data analytics methods must be identified to optimise the trade-off between benefit and side effects.

*4.3. Searchable Encryption.* Searchable encryption (SE) is a cryptographic technique that allows secure searching over encrypted data [32]. SE allows a user (or an automated program) to perform a secure query for a specific event without compromising the data confidentiality. For example, using SE to encrypt data on the cloud prevents the cloud provider or any unauthorised person (including the system administrator) from accessing or querying the encrypted data. There are two SE schemes [33]; one of these schemes is Symmetric Searchable Encryption (SSE). SSE requires a private key to be distributed between users, which is not suitable for multiple user scenarios [34]. The other scheme is Public Key Encryption with Keyword Search (PEKS) [35]. PEKS is a public-key cryptosystem that allows search over encrypted data using a public key instead of private keys, allowing multiple parties to query the data without compromising the data owner's private key.

*4.4. Access Control Methods.* There are several known AC mechanisms, including but not limited to attribute-based, key-policy-based, role-based, and trust-based [36]. However, the most commonly used AC mechanisms with PEKS are

role- and attribute-based access control. Table 2 summarises the difference between these two AC mechanisms, based on two recent publications [37, 38]. The following subsections will further discuss those approaches and their capacity to be combined with SE and critically compare them in the context of IIoT.

*4.5. Role-Based Access Control (RBAC) with PEKS.* RBAC is a security mechanism that allows users to access data based on their roles within an organisation [39]. The authors in [40] introduced RBAC to PEKS using free bilinear, as bilinears have high computational cost. The authors used the RBAC mechanism to simplify the frequent user's permission assignment within a large organisation. However, using RBAC with PEKS makes it hard to manage third parties' access policies (users outsides the organisation), which is an essential requirement for a monitoring system in the IIoT. Besides, using RBAC with PEKS is inflexible as it must be painstakingly managed.

*4.6. Attribute-Based Encryption (ABE).* Attribute-based access control (ABAC) is a security mechanism that allows organisations to grant access to users based on some attributes, such as their division or title [41]. On the other hand, Attribute-Based Encryption (ABE) combines searchable encryption with the ABAC approach [42]. In ABE, a message is encrypted for a specific receiver using a set of attributes. Thus, only the person who holds a key for the matching attributes can decrypt the message [39]. ABE has two paradigms: Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE). In KP-ABE, the user's private key is associated with a specified access policy, and the ciphertext is encrypted under a set of attributes. The user can decrypt the ciphertext if the attributes in ciphertext satisfy the access policy in the user's key. Thus, KP-ABE mechanism answers the following question, "what type of data should the user access?". Differently, the CP-ABE answers the question, "What attributes must a user have to access the encrypted data?". Typically, CP-ABE is considered an adjustable scheme because it guarantees more control to the user over the encrypted data [43].

Rasori [43] improved ABE and reduced the communication overhead by 35 per cent compared with existing ABE for medical applications. This novel CP-ABE is more efficient and could be a suitable solution for low-power communication protocols in IIoT. Sathya and Kumar [44] proposed a medical system that collects patient's data during emergencies and shares the data with the doctors. The authors' proposed system combines blowfish encryption and an ABE scheme. The authors evaluated their proposed system using several symmetric encryption algorithms, encryption time, decryption time, and total computation time. Their evaluation shows that the blowfish algorithm has better performance to encrypt data when used with CP-ABE to grant the authorised users' access to medical data. The main advantage of this work is the fast transmission of medical data, while the main disadvantage of using the blowfish algorithm is the linear relationship between the size of ciphertext and the number of attributes. When the number of attributes increases, so does the size of ciphertext.

Miao et al. [45] proposed a higher security level PEKS with CP-ABE approach that supports access control with multiple permissions as well as hidden access policies. Also, the authors employed traceability techniques to prevent dishonest data users from leaking their private key to others. Their evaluations show that the computation costs for encryption and decryption increase linearly as the number of user attributes does.

Yang et al. [46] proposed a system to monitor the patient's status with two access control modes. The first mode is for normal situations where the doctors, nurses, and technical staff have access under an access policy. The second mode is for emergencies where the first-aider needs access to the patient's historical data. To achieve these controlled access modes, the authors applied ABE for normal access and break-glass algorithm for emergency access. However, their approach provides data security but does not provide a revocation mechanism to the emergency access policy, once the situation is resolved.

*4.7. Attribute-Based Keyword Search (ABKS).* In the Attribute-Based Keyword Search (ABKS) scheme, the keywords are encrypted by an AC policy and the data with attributes. The user can generate a trapdoor that can be used to search over encrypted data [47]. The ABSE (attribute-based searchable encryption) scheme has exactly the contrary where the owner transmits the valid search query to the user and allows them to decrypt the data when its attributes satisfy the access policy [48]. However, ABKS schemes provide efficient search operations which allow retrieving encrypted data for multiple authorised users with flexible access policy [49].

Guo et al. [50] proposed a new ABKS to support encryption for both keyword and messages where most existing ABKS encrypts the keyword. In their proposed ABKS, there is no need for a secure channel to transmit the search tokens to the cloud. Also, it is a robust scheme against resisting offline keyword guessing attacks by inside attackers (i.e., the honest-but-curious servers). This scheme is evaluated and applied to a telemedicine system that is used to support healthcare services at multiple locations. However, the communication time in this scheme is high and is not suitable for time-sensitive applications.

*4.8. Combining Searchable Encryption with Access Control.* To achieve strong confidentiality, SE must be combined with access control [51, 52]: if a ciphertext appears as a search result, we learn something about the underlying document, even if the access control does not allow us to access the document. This illustrates the need for a linked search and access control, so that search results present to users only data to be accessed by the users [53]. Thus, the SE protects data confidentiality, and AC schemes protect user access privileges [54].

It is essential to protect data that travels through the IIoT network. Thus, SE covers cryptographic protection across all networks by (1) protecting the Edge and cloud networking and (2) protecting endpoint connectivity [9]. Encryption techniques protect the privacy of big data in the data storage phase. Confidentiality, the first consideration when the encrypted data is stored in cloud servers can be secured by

Table 2: Comparing role and attribute-based access control.

| Feature | Access control mechanism | |
|---|---|---|
| | Role-based access control (RBAC) | Attribute-based access control (ABAC) |
| Access control granularity | Coarse-grain access control | Fine-grain access controls |
| User addition mechanism | Creating access control groups defined as roles with presetup privileges. Users can be added into the group for their desired access privileges. | Users are assigned attributes to describe their properties. The access control system needs to focus on the required access control policies that are described by a set of attributes to check the user's privileges to decide if the access should be granted or not. |
| Structure of access policy | Policies are assigned (operation/object pairs) to groups before the access request is made. | Using Boolean rule structure to express the policies. |
| The input of authorisation decisions | Users are assigned to roles and inherit the permissions assigned to the roles they have. Roles are often organised in a role hierarchy, which defines the inheritance of permissions between roles. | They are used as input for authorisation decisions with many criteria, such as department, job code, time of day, IP address, and user location. |
| Decision level | Only related to functionality | Relate to access in both the data level and the field level, but also to functionality. |
| Access level | Do not allow access for nonemployees to organisation assets. | Allow limited access for third parties to organisational assets. |
| Model status | One of the main problems is that it is not an automatic model, needs to be painstakingly managed, and often involves significant manual intervention. The role-based mechanism, by itself, is inadequate to address the dynamic requirements of cloud-based IoT. | The ABAC model is a dynamic model. The system dynamically deploys access control by using attributes, i.e., a flexible access control approach. |

efficient encryption techniques. However, when the data user sends the request to retrieve the data from the cloud, the cloud server cannot reply to the user's request, because it cannot decrypt the encrypted data or search over encrypted data. Searchable encryption schemes could address these challenges.

While the Attribute-Based encryption (ABE) methods might secure information transmission and the fine-grained sharing of encrypted IIoT data, they additionally need to overcome new application deterrents in IIoT-cloud frameworks: (1) restricted resource IoT devices; (2) difficulty in encrypted data recovery at cloud servers: the encrypted records limit the adaptability and accuracy of information recovery, leading to unessential or incorrect outcomes; (3) lack of successful key administration: once CA is compromised, all previously encrypted files can be leaked because of the keys generated by a central authority (CA). To address the above difficulties, a novel lightweight searchable encryption method is needed for IIoT-cloud frameworks [55].

*4.9. Searchable Encryption with Access Control in IIoT Applications.* The literature survey of Zhou et al. [33], which spanned 2014 to 2019, identified schemes that combined PEKS with Attribute-Based Encryption (PEKS-ABE) for cloud-based applications. Moreover, this survey demonstrated that the PEKS-ABE provides efficient data sharing and searching ability, but it needs to improve the privacy of user keys. However, they do not also apply it to IIoT wherein to improve the privacy of the user keys, an Edge processing and storage approach could be utilised.

The following two works focus on improving either SE or AC for IIoT environments, but they do not combine them. Chen et al. [28] proposed lightweight searchable encryption for cloud-based IIoT applications with security improvements. In [56], published in 2020, they improve CP-ABE in many aspects:

(1) *Using a Hybrid Cloud Infrastructure*. Public cloud to store encrypted IoT data and the private cloud to execute CP-ABE tasks over the data

(2) *Guaranteeing Data Privacy at the User Level against the Private Cloud*. The author achieved this by proposing two encryption techniques. These techniques work by protecting IoT data privacy at the item level and preventing the user-key leakage problem.

(3) Enabling the private cloud to execute CP-ABE encryption/decryption tasks in batches and executing the CP-ABE reencryption tasks regardless of the size of IoT data, thus improving the performance of IIoT applications

Chen et al. [28] proposed lightweight searchable encryption for cloud-based IIoT applications with security improvements. To achieve more precise data retrieval, Miao et al. [57] proposed an improved ABE scheme with multikeyword search to support simultaneous numeric attribute comparison, thereby greatly enhancing the flexibility of ABE encryption in a dynamic IoT environment. Furthermore, attribute-based

multikeyword search schemes were also investigated in [58]. Nevertheless, this CP-ABE scheme inevitably concentrates on the single authority environment in which a CA essentially controls all attributes' authorisation. The single authorisation cannot effectively generate and manage the public/secret keys in the IIoT.

However, these studies did not improve the bandwidth of data that is outsourced to the cloud, which is important to minimise the computational cost. Zhang et al. [55] proposed a lightweight SE-AC scheme by providing lower computational complexity. Moreover, their framework enhanced privacy by preventing leakage during data outsourcing to a cloud server. In summary, they provide fine-grained AC, multikeyword search, lightweight decryption, and a multi-authority environment. They provide low latency as well as improved security against the chosen-keyword attack and the chosen-plaintext attack. Their LSABE and LSABE-MA schemes can support single keyword and multikeyword searching while maintaining the lightweight decryption on many practical testing platforms (PC, mobile phone, and Raspberry Pi models). Moreover, their schemes meet the low-latency requirement of IIoT applications. Therefore, their schemes are suitable for practical IIoT environments. However, their work did not consider the accuracy and data bandwidth, which is regarded as requirements of IIoT applications. In addition, the encryption time for their schemes is 24 seconds. Simultaneously, latency is an important metric in the encryption phase for the real-world IIoT environment. Thus, encrypted privacy-sensitive data must upload to the cloud immediately. Hence, we identify a gap in extracting the useful information from the raw data before encrypting them to minimise the encryption time and the bandwidth and to improve the overall performance to meet IIoT requirements.

## 5. Discussion

Several studies have combined SE with AC to query encrypted data with different AC policies. However, studies that combined PEKS and AC mechanisms, such as CP-ABE, still suffer from low privacy for user keys, high volumes of data transmission, or a high ratio of error for returned data (reduced accuracy). Some studies combined these algorithms in the medical domain to improve the privacy of medical data and the security level against external and internal attacks. Furthermore, some systems still have a high computational cost, which is not practical for a computationally restricted environment such as IIoT. This high computational cost prevents studies from meeting the real-time requirement for the time-sensitive IIoT applications. Therefore, IIoT applications must minimise the computational cost and improve performance to meet the near real-time requirements. Gebremichael et al. [19] discussed the further research that needs to be considered in the IIoT applications. The authors argue that using SE or homomorphic encryption (HE) can maintain security and privacy for systems that rely on cloud providers. Besides, SE provides fast and secure data delivery from the cloud for time-critical applications. Leading from the above discussion, we identify four research questions and open challenges as follows:

(i) *RQ1*. How do we adopt and deploy a lightweight version of the Public Key Encryption with Keyword Search (PEKS) algorithm on both the IIoT devices and the cloud to achieve a near real-time performance that is suitable for time-sensitive IIoT systems?

(ii) *RQ2*. How can we introduce, investigate, and evaluate the combination of PEKS and CP-ABE mechanisms in the cloud versus Edge architecture while achieving the best performance for time-sensitive IIoT systems?

(iii) *RQ3*. How do we investigate the performance overhead for deployment on the Edge vs. the cloud server on various IIoT applications and identify the proper architecture for each application type?

(iv) *RQ4*. How to design and develop a framework with an efficient CP-ABE mechanism and PEKS algorithm tailored to a suitable cloud and Edge deployment for IIoT systems to provide a secure and privacy-preserving solution for IIoT systems with AC support?

## 6. Conclusions

This study provided an unambiguous literature review that specifically focused on SE with AC for IIoT in a systematic manner. We demonstrated that the existing approaches and articles do not meet all the requirements of IIoT to support smart factory needs. Our review highlights the efficient combination between AC or CP-ABE and SE or PEKS to preserve privacy and minimise the execution time. These improvements can assist in taking smart decisions, specifically if deployed in an cloud-Edge architecture. However, the remaining open challenges need to be addressed to evaluate if these solutions can provide an efficient and reliable framework for IIoT applications.

## Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

## Acknowledgments

This work was supported by a scholarship through University of Tabuk in Saudi Arabia (TBU331). We would like to thank Dr. Jeremy Singer, Dr. Tim Storer, and Dr. Christos Anagnostopoulos for their feedback.

## References

[1] M. Hermann, T. Pentek, and B. Otto, "Design principles for Industrie 4.0 scenarios: a literature review," in *2016 49th Hawaii international conference on system sciences (HICSS)*, pp. 3928–3937, Koloa, HI, USA, 2016.

[2] Y. Yu, R. Chen, H. Li, Y. Li, and A. Tian, "Toward data security in edge intelligent IIoT," *IEEE Network*, vol. 33, no. 5, pp. 20–26, 2019.

[3] P. R. Newswire, *Global Industrial IoT Market: Research Report 2015-2019*, Lon-Reportbuyer, 2015.

[4] F. Roberts, *9 examples of manufacturers making IIoT work for them*, Internet of Business, 2016.

[5] C. Liu, F. Chen, J. Zhu, Z. Zhang, C. Zhang, and C. Zhao, *Industrial IoT Technologies and Applications, Vol. 202*, Springer International Pu, 2017.

[6] P. Mathur, *IoT Machine Learning Applications in Telecom, Energy, and Agriculture*, Springer Nature Switzerland AG, 2020.

[7] G. Drosatos, K. Rantos, D. Karampatzakis, T. Lagkas, and P. Sarigiannidis, "Privacy-preserving solutions in the Industrial Internet of Things," in *2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 219–226, Marina del Rey, CA, USA, May 2020.

[8] STHE Web and FORA-r Devices, *IoT FOR BUSINESS Take Manufacturing's Shift Your Manufacturing Shift to Lightspeed to Lightspeed*, 2020.

[9] J. Wan, J. Li, M. Imran, D. Li, and Fazal-e-Amin, "A blockchain-based solution for enhancing security and privacy in smart factory," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3652–3660, 2019.

[10] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "A systematic survey of Industrial Internet of Things security: requirements and fog computing opportunities," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 4, pp. 2489–2520, 2020.

[11] M. S. Hossain and G. Muhammad, "Cloud-assisted Industrial Internet of Things (IIoT) - enabled framework for health monitoring," *Computer Networks*, vol. 101, pp. 192–202, 2016.

[12] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in Industrial Internet of Things," in *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, San Francisco, CA, USA, June 2015.

[13] P. P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, and X. Yi, "Privacy preserving Internet of Things: from privacy techniques to a blueprint architecture and efficient implementation," *Future Generation Computer Systems*, vol. 76, pp. 540–549, 2017.

[14] H. F. Atlam, A. Alenezi, R. K. Hussein, and G. B. Wills, "Validation of an adaptive risk-based access control model for the Internet of Things," *International Journal of Computer Network and Information Security*, vol. 10, no. 1, pp. 26–35, 2018.

[15] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: challenges, opportunities, and directions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, 2018.

[16] L. Luo, Y. Zhang, B. Pearson, Z. Ling, H. Yu, and X. Fu, "On the security and data integrity of low-cost sensor networks for air quality monitoring," *Sensors*, vol. 18, no. 12, p. 4451, 2018.

[17] X. Yu and H. Guo, "A survey on IIoT security," in *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)*, pp. 1–5, Singapore, 2019.

[18] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: architecture, enabling technologies, security and privacy, and applications," *Ieee Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[19] T. Gebremichael, L. P. Ledwaba, M. H. Eldefrawy et al., "Security and privacy in the Industrial Internet of Things: current standards and future challenges," *IEEE Access*, vol. 8, pp. 152351–152366, 2020.

[20] K. Pothong, I. Brass, M. Carr et al., *Editors of the Cybersecurity of the Internet of Things: PETRAS Stream Report 03 Privacy and Trust 05 Adoption and Acceptability*, PETRAS Stream Report, 2019.

[21] P. Jayalaxmi, R. Saha, G. Kumar, N. Kumar, and T.-h. Kim, "A taxonomy of security issues in Industrial Internet-of-Things: scoping review for existing solutions, future implications, and research challenges," *IEEE Access*, vol. 9, pp. 1–1, 2021.

[22] A. Sciences, *Security and Privacy Trends in the Industrial Internet of Things*, Springer, Berlin, Germany, 2019.

[23] J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, article 102481, 2020.

[24] M. S. Virat, S. M. Bindu, B. Aishwarya, B. N. Dhanush, and M. R. Kounte, "Security and privacy challenges in Internet of Things," in *Proceedings of the 2nd International Conference on Trends in Electronics and Informatics*, pp. 454–460, Tirunelveli, India, 2018.

[25] T. Qiu, J. Chi, X. Zhou, Z. Ning, M. Atiquzzaman, and D. O. Wu, "Edge computing in Industrial Internet of Things: architecture, advances and challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2462–2488, 2020.

[26] I. Ungurean and N. C. Gaitan, "A software architecture for the Industrial Internet of Things—a conceptual model," *Sensors*, vol. 20, p. 5603, 2020.

[27] B. Chen, J. Wan, A. Celesti, D. Li, H. Abbas, and Q. Zhang, "Edge computing in IoT-based manufacturing," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 103–109, 2018.

[28] B. Chen, L. Wu, N. Kumar, K.-K. R. Choo, and D. He, "Lightweight searchable public-key encryption with forward privacy over IIoT outsourced data," *IEEE Transactions on Emerging Topics in Computing*, 2019.

[29] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. P. C. Rodrigues, "Authentication in cloud-driven IoT-based big data environment: Survey and outlook," *Journal of Systems Architecture*, vol. 97, pp. 185–196, 2019.

[30] X. Kong, J. Chang, M. Niu, X. Huang, J. Wang, and S. I. Chang, "Research on real time feature extraction method for complex manufacturing big data," *International Journal of Advanced Manufacturing Technology*, vol. 99, no. 5-8, pp. 1101–1108, 2018.

[31] T. P. Raptis, A. Passarella, and M. Conti, "Data management in industry 4.0: state of the art and open challenges," *IEEE Access*, vol. 7, pp. 97052–97093, 2019.

[32] K. Chamili, M. J. Nordin, W. Ismail, and A. Radman, "Searchable encryption: a review," *International Journal of Security and Its Applications*, vol. 11, no. 12, pp. 79–88, 2017.

[33] Y. Zhou, N. Li, Y. Tian, D. An, and L. Wang, "Public key encryption with keyword search in cloud: a survey," *Entropy*, vol. 22, no. 4, pp. 1–24, 2020.

[34] S. T. Hsu, C. C. Yang, and M. S. Hwang, "A study of public key encryption with keyword search," *International Journal of Network Security*, vol. 15, no. 2, pp. 71–79, 2013.

[35] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *2010 Proceedings IEEE INFOCOM*, San Diego, CA, USA, March 2010.

[36] R. Charanya and M. Aramudhan, "Survey on access control issues in cloud computing," in *2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)*, Pudukkottai, India, 2016.

[37] M. U. Aftab, Z. Qin, N. W. Hundera et al., "Permission-based separation of duty in dynamic role-based access control model," *Symmetry*, vol. 11, no. 5, p. 669, 2019.

[38] S. Bhatt, L. A. Tawalbeh, P. Chhetri, and P. Bhatt, "Authorizations in cloud-based Internet of Things: current trends and use cases," in *2019 4th International Conference on Fog and Mobile Edge Computing, FMEC 2019*, vol. 1, pp. 241–246, Rome, Italy, 2019.

[39] S. Shekhar and H. Xiong, "Geo-Role-Based Access Control," in *Encyclopedia of GIS*, pp. 368–368, Springer, 2008.

[40] K. Rajesh Rao, I. G. Ray, W. Asif, A. Nayak, and M. Rajarajan, "R-PEKS: RBAC enabled PEKS for secure access of cloud data," *IEEE Access*, vol. 7, pp. 133274–133289, 2019.

[41] P. J. Sun, "Privacy protection and data security in cloud computing: a survey, challenges, and solutions," *IEEE Access*, vol. 7, pp. 147420–147452, 2019.

[42] Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, "Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 12, pp. 2706–2716, 2016.

[43] M. Rasori, "*fABElous: an attribute-based scheme for Industrial Internet of Things*," in *2019 IEEE International Conference on Smart Computing (SMARTCOMP)*, Washington, DC, USA, June 2019.

[44] D. Sathya and P. G. Kumar, "Secured remote health monitoring system," *Healthcare Technology Letters*, vol. 4, no. 6, pp. 1–5, 2017.

[45] Y. Miao, X. Liu, K. K. R. Choo et al., "Privacy-preserving attribute-based keyword search in shared multi-owner setting," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, pp. 1–15, 2019.

[46] 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.

[47] Q. Zheng, S. Xu, and G. Ateniese, "VABKS: verifiable attribute-based keyword search over outsourced encrypted data," in *IEEE INFOCOM 2014-IEEE conference on computer communications*, pp. 522–530, Toronto, ON, Canada, May 2014.

[48] H. Yin, J. Zhang, Y. Xiong et al., "CP-ABSE: a ciphertext-policy attribute-based searchable encryption scheme," *IEEE Access*, vol. 7, pp. 5682–5694, 2019.

[49] Q. Li, Y. Yue, and Z. Wang, "Deep Robust Cramer Shoup Delay Optimized Fully Homomorphic for IIOT secured transmission in cloud computing," *Computer Communications*, vol. 161, pp. 10–18, 2020.

[50] L. Guo, Z. Li, W. C. Yau, and S. Y. Tan, "A decryptable attribute-based keyword search scheme on eHealth cloud in Internet of Things platforms," *IEEE Access*, vol. 8, pp. 26107–26118, 2020.

[51] Y. W. Hwang, I. Y. Lee, and K. Yim, "A study on access control scheme based on ABE using searchable encryption in cloud environment," in *Advances in Internet, Data and Web Technologies*, vol. 47 of Lecture Notes on Data Engineering and Communications Technologies, pp. 215–221, 2020.

[52] D. Ziegler, A. Marsalek, B. Prünster, and J. Sabongui, "Efficient access-control in the IIoT through attribute-based encryption with outsourced decryption," in *Proceedings of the 17th International Joint Conference on e-Business and Telecommunications: SECRYPT*, Portugal, 2020.

[53] N. Löken, "Searchable encryption with access control," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, Reggio Calabria, Italy, 2017.

[54] P. Chaudhari and M. L. Das, "Privacy preserving searchable encryption with fine-grained access control," *IEEE Transactions on Cloud Computing*, vol. 7161, no. c, pp. 1–1, 2019.

[55] K. Zhang, J. Long, X. Wang, H.-N. Dai, K. Liang, and M. Imran, "Lightweight searchable encryption protocol for Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 4248–4259, 2021.

[56] S. Qi, Y. Lu, W. Wei, and X. Chen, "Efficient data access control with fine-grained data protection in cloud-assisted IIoT," *IEEE Internet of Things Journal*, vol. 4662, no. c, pp. 1–1, 2020.

[57] Y. Miao, J. Ma, X. Liu, X. Li, Z. Liu, and H. Li, "Practical attribute-based multi-keyword search scheme in mobile crowdsourcing," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 3008–3018, 2018.

[58] Y. Miao, X. Liu, R. H. Deng et al., "Hybrid keyword-field search with efficient key management for industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3206–3217, 2019.