future internet

MDPI

Review

Risk-Based Access Control Model: A Systematic Literature Review

Hany F. Atlam [1,2,*], Muhammad Ajmal Azad [3], Madini O. Alassafi [4], Abdulrahman A. Alshdadi [5] and Ahmed Alenezi [1,6]

[1] Electronic and Computer Science Department, University of Southampton, Southampton SO17 1BJ, UK; aa4e15@soton.ac.uk
[2] Computer Science and Engineering Department, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
[3] Department of Engineering and Technology, University of Derby, Derby DE22 1GB, UK; m.azad@derby.ac.uk
[4] Department of Information Technology, Faculty of Computing and IT, King Abdulaziz University, Jeddah 21589, Saudi Arabia; malasafi@kau.edu.sa
[5] Department of Information Systems and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah 23218, Saudi Arabia; Alshdadi@uj.edu.sa
[6] Computer Science Department, Faculty of Computing and Information Technology, Northern Border University, Arar 9280, Saudi Arabia
* Correspondence: hfa1g15@soton.ac.uk; Tel.: +44-7422523772

Received: 1 May 2020; Accepted: 3 June 2020; Published: 11 June 2020

Abstract: Most current access control models are rigid, as they are designed using static policies that always give the same outcome in different circumstances. In addition, they cannot adapt to environmental changes and unpredicted situations. With dynamic systems such as the Internet of Things (IoT) with billions of things that are distributed everywhere, these access control models are obsolete. Hence, dynamic access control models are required. These models utilize not only access policies but also contextual and real-time information to determine the access decision. One of these dynamic models is the risk-based access control model. This model estimates the security risk value related to the access request dynamically to determine the access decision. Recently, the risk-based access control model has attracted the attention of several organizations and researchers to provide more flexibility in accessing system resources. Therefore, this paper provides a systematic review and examination of the state-of-the-art of the risk-based access control model to provide a detailed understanding of the topic. Based on the selected search strategy, 44 articles (of 1044 articles) were chosen for a closer examination. Out of these articles, the contributions of the selected articles were summarized. In addition, the risk factors used to build the risk-based access control model were extracted and analyzed. Besides, the risk estimation techniques used to evaluate the risks of access control operations were identified.

Keywords: access control; security risk; risk-based access control; risk estimation techniques; risk factors; systematic review

1. Introduction

Security is the nightmare for almost all new technologies. Providing a secure system is not an easy task. One of the significant components to resolve security challenges is to build an efficient and effective access control model. This model is utilized to manage access to system resources by allowing only authorized users who have been authenticated successfully. An access control model

comprises three main items: subject, target and rules. Subjects are system users who make the access request to access system resources (targets). Rules are utilized to make the access decision, whether granting or denying access [1,2]. The main purpose of the access control is to decline unauthorized users and reduce the tasks of authorized users on a certain device. In addition, it prevents the action that could trigger a security violation [3].

There are two classes of access control approaches: traditional and dynamic. Traditional access control approaches utilize rigid and predetermined policies to determine the access decision. These static policies provide the same decision in different circumstances. Therefore, this inflexible approach cannot provide a robust security method for various dynamic and distributed systems such as the Internet of Things (IoT) and cloud computing [4]. Alternatively, dynamic access control methods employ not only static policies but also dynamic and real-time features to make access decisions. These dynamic features can involve context, trust, history events, location, time, and security risk [5].

Risk-based access control model is one of the dynamic methods that utilize the security risk value related to each access request as a criterion to determine access decisions [1]. A risk-based access control model provides several benefits over current access models. For example, it delivers more flexibility and resilience while accessing system resources by utilizing dynamic and contextual features to determine the access decision. In addition, it considers the exceptional and unpredicted access requests that are essential for some applications such as healthcare and the military, where granting access can literally save thousands of lives [6]. The ultimate goal of the risk-based access control model is to produce a scheme that promotes information sharing to increase the organization's benefit and at the same time keeps users responsible for their activities and stops the anticipated damage due to sensitive information disclosure [4].

The objective of the paper is to present a systematic literature review and investigate the state-of-the-art of the risk-based access control model, which is one of the pillars toward designing a dynamic and adaptive access control model for distributed systems. Based on the selected search plan, 44 articles (of 1044 articles) were chosen for closer investigation. Out of the retrieved and analyzed articles, the risk factors utilized to design the risk-based access control model were extracted and analyzed. Besides, the risk estimation techniques used to evaluate security risks were identified. In addition, the contributions of the selected articles were summarized. As compared to other surveys, to the best of the authors' knowledge, this is the first paper that provides a systematic literature review for the risk-based access control model.

The contribution of this paper can be summarized as follows:

- Reviewing recent studies of risk-based access control models by providing a summary of the contributions of each study.
- Identifying and analyzing various risk factors used in recent risk-based access control models.
- Determining and investigating different risk estimation techniques utilized in recent risk-based access control models.

The rest of this paper is structured as follows. Section 2 gives an overview of access control approaches; Section 3 introduces the risk-based access control model and its main components; Section 4 provides the research methodology; Section 5 presents the analysis of results; Section 6 presents a discussion to show how this systematic review answered proposed research questions, and Section 7 is the conclusion.

2. An Overview of Access Control

The key objective of the access control is to limit operations performed by authorized users. In addition, it prohibits any action that could trigger a security violation [1]. An effective access control model should fulfill the security demands of confidentiality, integrity, and availability [3]. It is essential to make a reasonable distinction between authentication, authorization, and access control. Authentication is the process of verifying the identity of a user [7], while allowing or denying access to an authenticated user to carry out particular tasks on particular resources is called authorization.

Access control is the process of enforcing authorization policies. Once a user is authenticated and the authorization level is identified, access control is used to enforce user permissions to prevent the user/subject from accessing anything that he/she should not be able to [3].

The history of the phrase "Access Control" has started in transportation in the first half of the 20th century. The concept of the limited-access road was suggested in 1907 to control fast-growing motor traffic. Although early cars were not as fast as today's standard, car drivers were enforced to control their speed on highways. They were enforced to enter and exit via one-way ramps to control the access to highways, which led to a reduction in the probability of cross-traffic accidents and increases the speed of traffic flows [8].

Currently, access control is applied at diverse levels in several domains such as database management systems and operating systems to control resources and allow only legal users/subjects to use system resources in an authorized way. An access control model comprises of five core elements: subjects, actions, objects, privileges, and access policies [9].

- **Subjects**: represents various entities that can be user, agents, or processes that make an access request to access system resources (objects).
- **Objects**: describes system resources encompassing data or information that needed to be accessed by subjects/users.
- **Actions**: represents various types of actions or activities that subjects can perform on a particular object such as read, write, execute, etc.
- **Privileges**: These are the permissions that are granted to subjects to be able to carry out a particular action on a particular object.
- **Access policies**: These are a group of rules or procedures that specify the criteria needed to determine the access decision whether granting or denying access for each access request.

The flow of an access control process can be shown in Figure 1. The flow begins when a subject/user sends an access request to the access control manager to access a particular object. Then, the access control manager compares the subject's credentials against access policies to decide whether granting or denying access. If the access is granted, the access control manager will allow the user to access the object. While if the access is denied, the access control manager will send a warning message due to insufficient credentials and ask the subject to use sufficient credentials to be able to access the requested object [9].

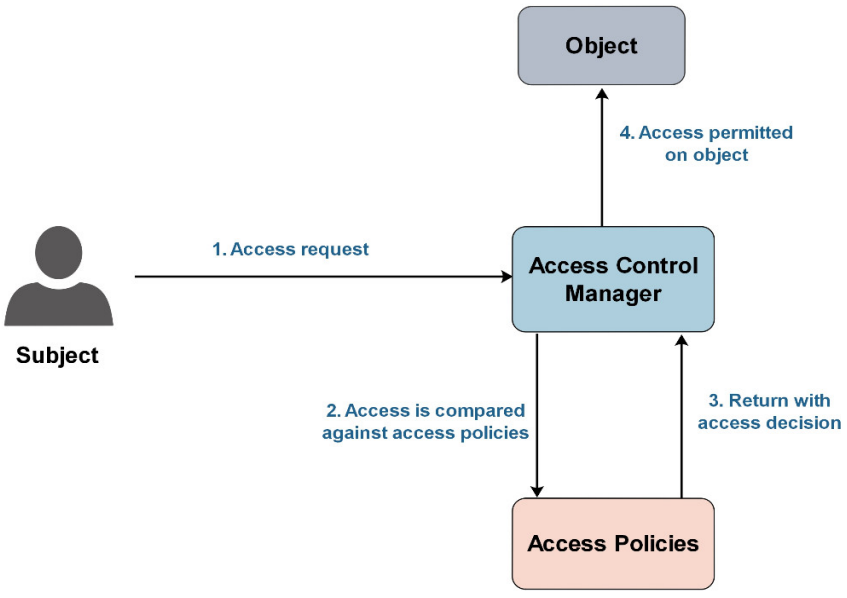

Figure 1. Flow of an access control operation.

There are many access control approaches, which can be categorized into two main groups: traditional and dynamic access control approaches.

2.1. Traditional Access Control Models

Traditional access control (also called classical or static) approaches utilize rigid and predetermined policies to determine the access decision. These static and rigid policies provide the same decision in different circumstances. Although traditional access control approaches were successfully applied in different environments to solve various problems, these approaches are designed to provide a relationship between information associated with an access control rule logic and a resource for which access is requested. The implementation of an access control approach is subject to manipulation, which can range from an unexpected situation, including poorly written access policies to several malicious entities acquiring access to a set of existing accounts. Therefore, traditional access control approaches provide a set of advantages, but they also have drawbacks. One of these drawbacks is that it cannot handle unpredicted situations as they are based on static and predefined policies [10]. This inflexible approach cannot provide a robust security method for various dynamic and distributed systems such as IoT and Cloud Computing, which need more flexibility in accessing system resources. Instead, this static approach can be the best solution in situations where there is no way to collect a contextual feature/attribute while making the access request, for example the operating system.

There are various traditional access control approaches including Access Control List (ACL), Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC). ACL is a list of specific objects that involve lawful users together with their access permissions. ACLs are utilized in various systems, for example, UNIX systems. Although ACL is an efficient and effective model, it is not scalable, in which it cannot cope with a huge list of objects and subjects. For DAC, it is mainly built for multi-user databases and systems with few previously known users. Granting access in DAC is mainly based on the subject identity and authorization that are determined using open policies. This enables the object's owner to allow access to this object to any subject. For MAC, the level of sensitivity of objects is used to categorize objects into several sensitivity levels—for example, sensitive, not sensitive, confidential, etc. Each object has a label that specifies the sensitivity level of that object. In addition, each subject has a label that specifies the object the subject can access [11,12]. For RBAC, it involves three main components: users or subjects, roles (collections of permissions), and actions (activities performed on target resources) [13]. The basis of RBAC depends on roles, in which each role is accompanied by a set of access permissions. Each organization has several roles—for example, client, employee, manager, administrator, etc. A user can be a member of one or more roles, and a role can involve one or more users [14].

2.2. Dynamic Access Control Models

The core principle of dynamic access control models is that they consider not only access policies but also dynamic and contextual features that are collected at the time of the access request to make access decisions [15]. This provides more flexibility and can adjust to various situations and circumstances while making the access decision.

The need to adopt dynamic access control approaches should be one of the essential priorities to provide efficient and flexible access control model. However, most existing access methods are relying on static and rigid access policies and manual processes. These approaches are unable to provide a roadmap to improve automation significantly. This absence of automation results in a heavy involvement of human analysis that is error-prone and susceptible to various types of attacks based on social engineering. Additionally, current classical approaches have issues with resolving risks and threats in real time, especially when handling a previously unidentified threat. This is because these approaches make their access decision based on a set of policies built by a security analyst, who cannot resolve different access control situations in real time but can deal only with problems that were recognized before [16].

Instead of static policies, dynamic access methods use dynamic and real-time features to provide access decisions. These dynamic features can include trust, context, history, risk and operational need. Besides, these dynamic methods can adapt to different situations and circumstances at the time of deciding access decisions [5,17]. This dynamic access control approach can be valuable for several applications such as healthcare and the military, where considering exceptional access requests to provide the access can literally save thousands of lives. Table 1 provides a comparison between traditional and dynamic access control approaches.

Table 1. Comparison between traditional and dynamic access control approaches. ACL: Access Control List, DAC: Discretionary Access Control, IoT: Internet of Things, MAC: Mandatory Access Control, and RBAC: Role-Based Access Control.

Item	Traditional Access Control	Dynamic Access Control
Features	It uses predetermined and static policies to determine the access decision.	It uses access policies and contextual features that are collected at the time of making the access request to determine the access decision.
Grant Decision	The access is granted only if it matches one of the rules in the access policy.	The access is granted based on the context and the policy. The decision can be overridden based on the context.
Deny Decision	The access is denied only if it does not match any rule in the access policy.	The access is denied based on the context and the policy. The change in the context can lead to changing the decision immediately.
Example	ACL, DAC, MAC, and RBAC are the common and popular approaches or examples of traditional access control.	Risk-based access control, trust-based access control, and combination of risk with trust are common examples of dynamic access control.
Advantages	• Easy to understand, test, and maintain. • Faster to be produced. • Objective method, so the outcome is more accurate. • No contextual data is required, so it faster in making access decisions.	• Adapt to unpredicted situations and conditions that policies cannot expect. • Improve flexibility while accessing system resources. • Resolving risks and threats in real time, especially when handling a previously unidentified threat. • Can literally save lives in healthcare and military applications.
Weaknesses	• Cannot adapt to changes in situations and circumstances, which affect flexibility. • The policy is imperfect and do not have a plan for all contingencies, so many problems may arise. • Not a scalable solution especially with a large number of users and objects. • Hard to modify/update access rights for individual users.	• More complex, especially with many contextual attributes. • Contextual features are varied based on the domain/field. • Hard to identify effective contextual features for the access control model. • Subjectivity in assigning a weight for each contextual feature. • Time overhead for processing dynamic features with the policy. • Need more computing power.
Applications	The applications that do not have access to real-time features/attributes such as the operating system.	Various dynamic and distributed systems need dynamic access control to provide more flexibility including IoT and cloud applications, etc.

The security risk is one of the dynamic features that is used to build a risk-based access control model. The next section provides an overview of the risk-based access control model.

3. Risk-Based Access Control Model

Commonly, the risk is the possibility of loss or injury. It is about some incident that may arise in the future and cause losses. According to Elky [18], the risk is defined as "*the possible damage that may arise from the existing operation or from some upcoming incident*". The risk is found in numerous domains of our life. From the information technology security perspective, the security risk is defined as the damage that undesirably affects operation and its related information, while the process of understanding and mitigating against issues that may result in a breach of confidentiality, integrity, or availability of an information system is called risk management [18].

Security risk in the access control context can be defined as the possibility of information leakage and the value of this information that may occur from accessing system resources [1]. Risk-based access control model utilizes the security risk as a criterion to make the access decision for each access request. This model is based on estimating the security risk value associated with each access request dynamically, and it then uses the estimated risk value to decide whether granting or denying access [4]. Mathematically, the most popular formula to represent the risk in a quantitative form is the likelihood/ probability of an incident to occur multiplied by the impact regarding that incident [19].

There are several methods to build a risk-based access control model. These methods have certain common features from different models. The main elements of a risk-based access control model are shown in Figure 2. The risk-based access control model comprises three key modules. The risk estimation is the main module, which gets access requests from users, analyzes them, collects the required information of risk factors, and estimates the security risk value related to each access request. Then, the estimated risk value is compared against access policies to decide the access decision whether granting or denying the access [20].

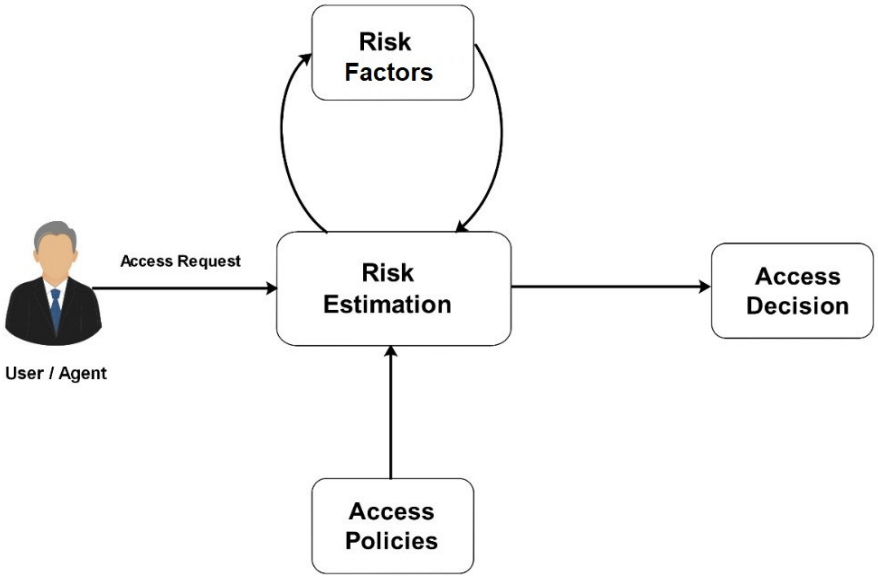

Figure 2. Main elements of a risk-based access control model.

4. Methodology

The risk-based access control model has several advantages in terms of flexibility and ability to provide an effective security model for dynamic systems. This systematic literature review is conducted to examine and investigate current research regarding risk-based access control models and explain the findings of the conducted review. A systematic literature review is mainly conducted as a way to specify, evaluate, and interpret all available research related to specific research questions, certain subjects, or phenomenon of interest [21].

Conducting a systematic literature review passed through five stages, as depicted in Figure 3. The first stage aims to formulate the research questions that the current review paper attempts to answer and then decide the criteria to include or exclude articles in the second stage to make sure

that the selected articles are the best and most appropriate regarding the review objectives. The third stage is the main stage that discusses at length which different databases will be searched to locate relevant articles. The fourth stage analyzes the results and then in the fifth stage, the results of each research question will be discussed.

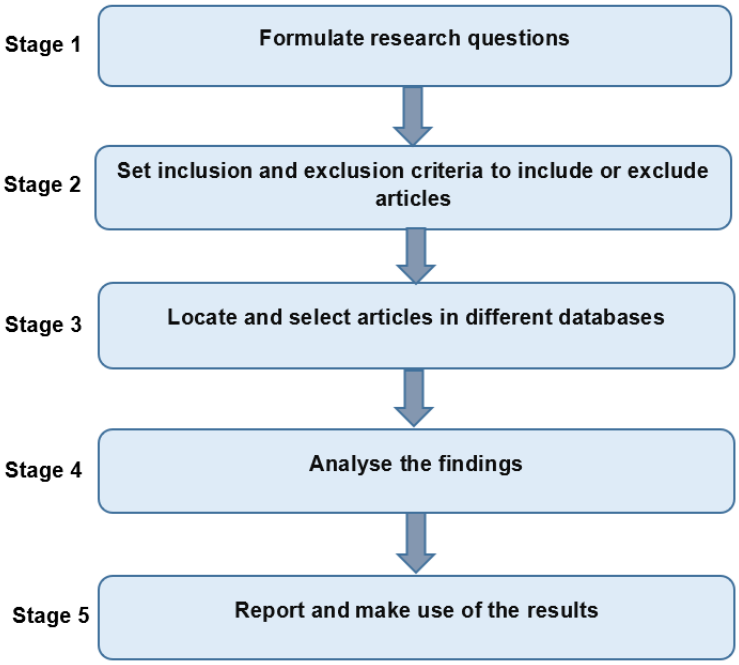

Figure 3. Stages of the current systematic literature review.

This approach/methodology was adopted to make the reader fully aware of the stages of conducting this systematic literature review. The methodology was started by defining the research questions to have a specific target while reviewing multiple publications. Then, inclusion and exclusion criteria were presented to show how the retrieved publication are filtered to reach the target of the study. Data sources where publications were retrieved are also presented to show the digital libraries utilized to collect these publications. In addition, the selection of relevant articles is discussed. The adopted methodology has several advantages in which it aims to describe the full process utilized to reach the target of the study to make the reader fully aware of all the procedures conducted by the researcher. In addition, this approach was adopted in several previous systematic literature reviews. On the other hand, this approach produces some drawbacks in which it limits the scope of the review/study, which may not give all the information about a certain topic to the reader.

4.1. Research Questions

The current study/paper aims to answer the subsequent research questions:

- RQ1: What are recent and peer-reviewed literature regarding risk-based access control models?
- RQ2: What are the risk factors used to build risk-based access control models?
- RQ3: What are risk estimation techniques employed in risk-based access control models?

4.2. Inclusion and Exclusion Criteria

Inclusion and exclusion criteria for selecting the appropriate research were employed. These criteria are mainly aimed to answer research questions and ensure designing efficient literature review. Inclusion criteria were:

- Scientific and peer-reviewed articles
- Topic is mainly risk-based access control model
- Relevant to research questions

- Articles written in English
- Published any time (year of publication is open and is not limited to a specific period)

Exclusion criteria were:

- Articles concerning risk estimation techniques that are not in the context of risk-based access control models
- Articles concerning risk factors that are not in the context of risk-based access control models
- Unpublished articles, non-peer-reviewed articles, and editorial articles
- Articles that are not fully available
- Non-English articles
- Duplicates of already included articles

4.3. Data Sources

Searches were carried out via digital libraries. This systematic review involved the following electronic databases:

- IEEE Xplore
- PubMed
- Elsevier ScienceDirect
- Google Scholar
- ACM Digital Library
- SpringerLink.

A keyword-based search was employed to collect the articles that relevant to the topic and research questions. The main keywords that were utilized involve:

- Risk-Based Access Control
- Risk Estimation
- Risk estimation Technique
- Risk Factors
- Security Risk.

4.4. Selection of Relevant Articles

Selecting relevant and recent studies with respect to the risk-based access control model started with 1044 articles collected from various online digital libraries that were decided in the previous section. The selection process on the collected publications was divided into three phases:

- **Phase 1**: The results of the search and collected publications were filtered depending on the inclusion and exclusion criteria that were discussed in Section 4.2. The search conducted was not bounded by a specific range of years to be able to collect all relevant publications regarding risk-based access control models.
- **Phase 2:** The publications collected from various online digital libraries were assessed depending on the relevance of the publication to the topic and research questions by examining only the title and abstract.
- **Phase 3**: The main purpose of this phase was to remove the duplicates of the collected publications from six different online digital libraries.

5. Analysis of Results

The inclusion and exclusion criteria were applied on the collected publications through three phases, as depicted in Figure 4. Based on the assessment through reading only the title and the abstract and its relevance to the research questions, 986 publications were excluded. In addition, the duplicates between different online digital databases were excluded, in which 32 duplicate publications were excluded.

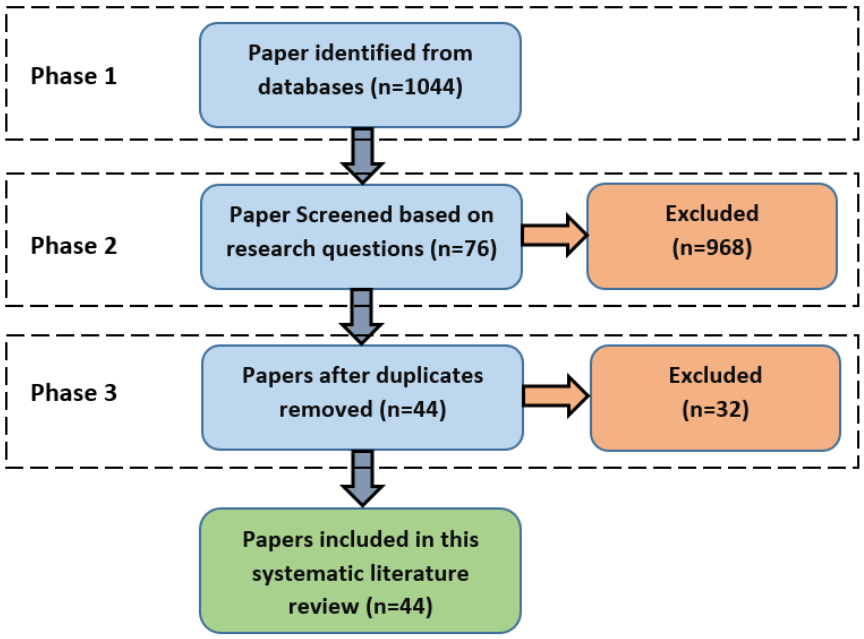

Figure 4. Flow diagram of the search.

The search that was executed in six different well-known online databases enables us to collect, as much as possible, most of the publications that are relevant to risk-based access control models. The result of the collected publications from each online database and the resultant number of publications after applying the three selection phases can be shown in Table 2. The results show that Google Scholar was the richest data source of publications related to risk-based access control models.

Table 2. The number of search result per database after applying three phases of the selection process.

Database	Phase 1	Phase 2	Phase 3
IEEE Xplore	16	9	4
PubMed	52	10	5
Google Scholar	886	37	28
SpringerLink	48	7	2
Elsevier ScienceDirect	22	8	3
ACM Digital Library	20	5	2
Total	**1044**	**76**	**44**

In addition, Figure 5 illustrates the number of articles published per year. The results show that the risk-based access control model started to attract the attention of the researcher after 2010. However, it is still an undiscovered area for multiple researchers. Given the steady number of publications in 2011, 2012, and 2013, we can see that the number of publications started to decrease, which reaches only one in 2019.

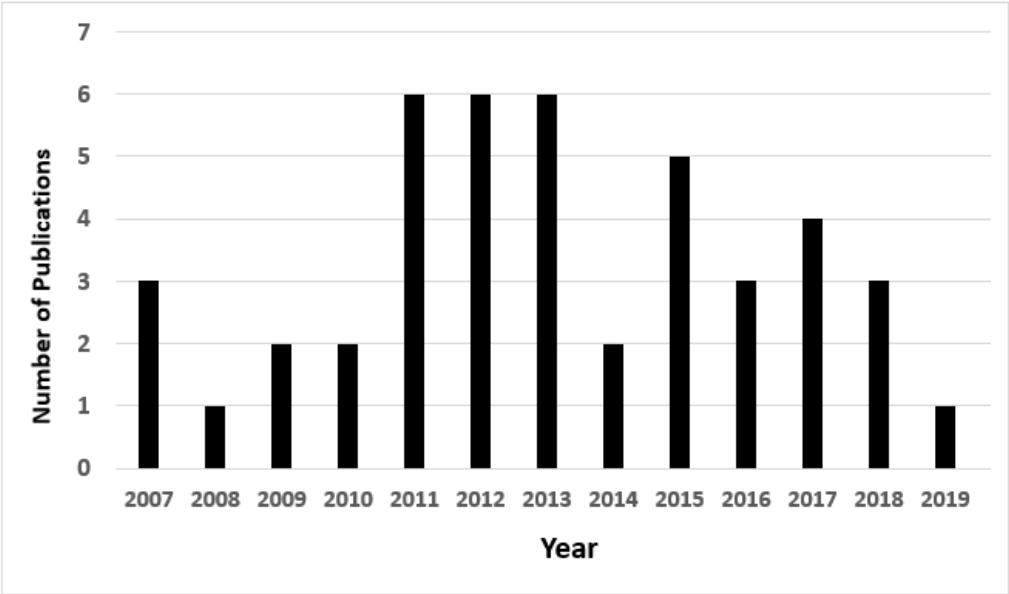

Figure 5. Number of selected articles published per year.

In addition, Figure 6 categorizes retrieved publications regarding risk-based access control models into either journal or conference publication per year. The results show that most publications that match our research questions were conference publications. In addition, Table 3 contains basic information about the analyzed and selected publications, which involve a publication's ID, publication citation, publication type, and year of publication. All selected/retrieved articles were published in peer-reviewed journals and conference proceedings. Besides, the selected publications contain only 3 book chapters, which are also peer-reviewed.

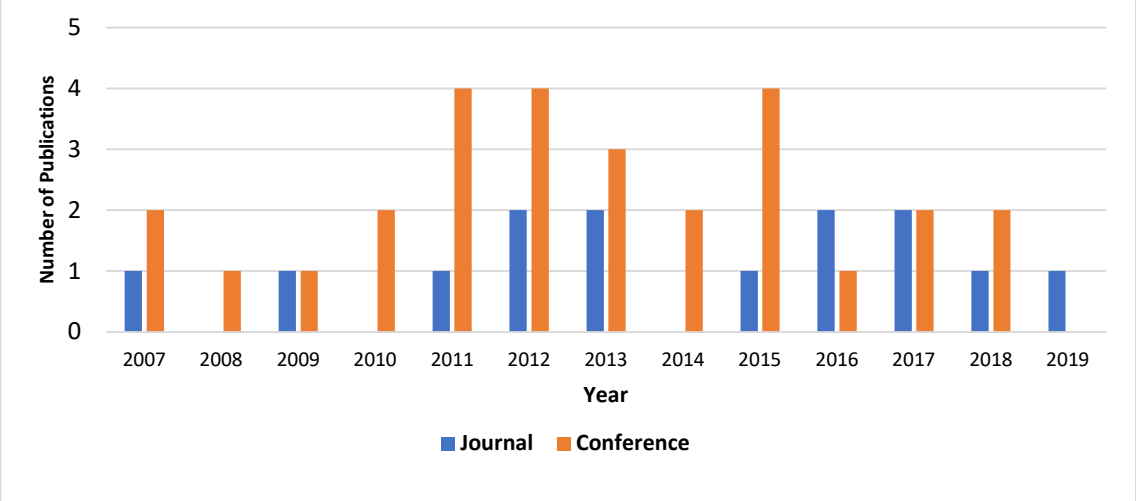

Figure 6. Number of journal and conference publications per year.

Table 3. Retrieved publications that are related to research questions.

Publication ID	Citation	Publication Type	Year of Publication
1	Ricardo et al. [22]	Journal	2016
2	Chen et al. [4]	Conference	2007
3	Diep et al. [20]	Conference	2007
4	Dos Santos et al. [1]	Conference	2014
5	Choi et al. [23]	Journal	2015
6	Khambhammettu et al. [6]	Journal	2013
7	Li et al. [24]	Conference	2013
8	Arias-Cabarcos et al. [25]	Journal	2012
9	Baracaldo and Joshi [26]	Journal	2013
10	Kandala et al. [27]	Conference	2011
11	Lee et al. [28]	Journal	2007
12	Atlam and Wills [29]	Journal	2019
13	Diaz-Lopez et al. [30]	Journal	2016
14	Shaikh et al. [5]	Journal	2012
15	Wang and Jin [15]	Conference	2011
16	Namitha et al. [31]	Conference	2015
17	McGraw et al. [32]	Journal	2009
18	Molloy et al. [33]	Conference	2011
19	Ni et al. [34]	Conference	2010
20	Abie and Balasingham [35]	Conference	2012
21	Shaikh et al. [36]	Conference	2011
22	Dos Santos et al. [37]	Conference	2013
23	Molloy et al. [38]	Conference	2012
24	Rajbhandari and Snekkenes [39]	Book Chapter	2011
25	Sharma et al. [40]	Conference	2012
26	Atlam et al. [41]	Conference	2017
27	Atlam et al. [42]	Journal	2018
28	Atlam et al. [43]	Conference	2017
29	Molloy et al. [44]	Conference	2009
30	Babu and Bhanu [45]	Conference	2015
31	Clark et al. [46]	Conference	2010
32	Helil et al. [47]	Journal	2011
33	Badar et al. [48]	Book Chapter	2013
34	Bijon et al. [13]	Conference	2013
35	Metoui et al. [49]	Conference	2016
36	Atlam et al. [9]	Conference	2018
37	Chun and Atluri [50]	Book Chapter	2008
38	Rahmati et al. [51]	Conference	2018
39	Metoui et al. [52]	Journal	2017
40	Burnett et al. [53]	Conference	2014
41	Dankar et al. [54]	Journal	2017
42	Abomhara et al. [55]	Journal	2015
43	Armando et al. [56]	Conference	2015
44	Chen and Crampton [57]	Conference	2012

6. Discussion

The risk-based access control model is one of the hot topics that many scholars are investigating to provide flexible, dynamic, and operative access control approach in distributed and dynamic systems. This paper can be a good starting point for such researchers to understand this model and review existing work related to proposed research questions. In this section, a discussion of the retrieved/analyzed publications was presented to show how the retrieved publications answered the proposed research questions.

RQ1: What are recent and peer-reviewed literature regarding risk-based access control models?

To answer this research question, retrieved/analyzed publications that are related to risk-based access control models will be discussed. Recent and peer-review publication outlined risk-based access control models are discussed. Table 4 summarizes the contributions of each publication.

Table 4. Summary of recent studies outlined risk-based access control models.

Citation	Summary of the Contributions of Each Publication
Chen et al. [4]	This paper presented a risk-based model that is based on the Multi-Level Security (MLS) approach. The paper utilized the risk value resulted from the difference between object and subject security level as a risk factor. Then, the fuzzy logic system was applied to represent the risk as a binary value, where 0 allows the access and 1 denies the access.
Diep et al. [20]	This paper presented the main elements needed to build a dynamic and flexible risk-based access control model by collecting environmental information, assess it, and make the access decision using a risk assessment.
Ni et al. [34]	This paper used the same elements of the risk-based model proposed by Diep et al. [20] but with the use of the fuzzy logic system to estimates the risk value associated with the access request. They indicated that the fuzzy logic system is an efficient method for evaluating the security risks of access control operations. The major difference between both publications was the risk estimation technique adopted to assess the security risk of each access request.
Lee et al. [28]	This paper provided a risk-based model by utilizing the risk assessment. The authors collected environmental and contextual information and assessed it based on outcomes of actions in term of CIA (Confidentiality, Integrity, and Availability). In addition, the MultiFactor Evaluation Process (MFEP) technique was utilized with the risk assessment to estimate the security risk value related to each access request to decide the access decision.
Chun and Atluri [50]	This paper proposed a risk-based model that employs the concept of "access first and verify later"; hence, the required information/data can be accessed immediately without delaying access. The paper also utilized semantics to build situation role hierarchies, which are used to assess the security risk to provide access decisions.
McGraw et al. [32]	This paper proposed a Risk-Adaptable Access Control (RAdAC) model, which is based on estimating the security risk and operational needs to grant or deny access. This model was implemented to first estimate the risk associated with the access request then compares the estimated risk with the access control policy. After that, the system verifies the operational needs, if the associated operational needs and the policy are met; then, the access is granted.
Kandala et al. [27]	This paper utilized the Risk-Adaptable Access Control (RAdAC) model developed by McGraw et al. [32] to identify different risk components with the operational needs using the Attribute-Based Access Control (ABAC) model. This paper integrated the ABAC model with the risk-based model to use other user attributes as risk factors.

Molloy et al. [44]	This paper reviewed open problems in risk-based access control systems and proposed using market approaches to identify the risk allocation and tolerance for each organization. The paper utilized the simulation to show the advantages of risk-based access control that promote security and information sharing.
Clark et al. [46]	This paper presented a risk-based access control model and how it can overcome issues with uncertainty and time-varying security specifications. The paper utilized resource sensitivity as a probability distribution, security labels, and clearance level to estimate the risk using the fuzzy logic system in various real-world situations.
Helil et al. [47]	This paper introduced a trust and risk-based access control model by combining trust and risk as risk factors to enhance data protection and information accessibility. Each user's trustworthiness and their related risk values were employed to decide the access decision.
Molloy et al. [33]	This paper presented a new learning and risk-based architecture for distributed policy enforcement under uncertainty. The paper utilized learned classifiers of access control decisions to improve the accuracy of the access decision.
Rajbhandari and Snekkenes [39]	This paper introduced a risk-based model that utilizes user's benefits rather than subjective probability as a risk factor to decide the access decision. The authors demonstrated that game theory can be used as a risk estimation approach to assess security risks.
Shaikh et al. [36] and Shaikh et al. [5]	The paper [36] proposed a dynamic risk-based decision method. This method used the user past behavior with the risk history to estimates the security risk value associated with each access request. Besides, it gave reward and penalty points for subjects/users after completing a transaction based on the estimated risk value associated with the transaction. The work presented in [36] was extended in [5] to involve the process of implementing the risk estimation process to identify good and bad users based on their past behavior.
Wang and Jin [15]	This paper proposed a quantified risk-based model. The risk value is estimated based on the purpose of access to different data sensitivity levels. The risk estimation process was performed by employing the concept of Shannon entropy from information theory. A prototype using medical history records was utilized to illustrate the efficiency of their suggested model.
Abie and Balasingham [35]	This paper implemented the concept of security risks to identify access decisions by proposing a risk-based adaptive security framework that employs the game theory as the risk estimation method to asses risk loses and their future benefits by collecting contextual information in the healthcare environment.
Arias-Cabarcos et al. [25]	This paper utilized the risk-based access control model in the federated identity management process in cloud computing. It utilized the security risk to provide the access decision and diminish weaknesses and risks when access decisions about collaboration are made. The paper also proposed a hierarchical risk aggregation system for cloud federation.
Chen and Crampton [57]	This paper incorporated the security risk with RBAC to build a risk-aware role-based access control model. In addition, the paper discussed the issues in the proposed risk-aware model and its implementation procedures.
Molloy et al. [38]	This paper utilized the risk-based access control model to make access decisions by utilizing the benefits of access as a risk factor. The paper also proposed an improved model that uses learned classifiers to provide efficient and accurate access decisions.
Sharma et al. [40]	This paper presented a task-based access control model that estimates the risk value based on the action to be performed by the requester. The risk estimation process evaluates the risk using outcomes of actions to make the access decision.

Baracaldo and Joshi [26]	This paper proposed a framework that extends the RBAC model to incorporate trust with risk to provide the access decision. The authors argued that their framework can be adjusted to different changes in users' behavior by using a threshold value that is defined using a risk assessment process.
Badar et al. [48]	This paper proposed utilizing classification to assess the risk value related to each access request. The paper presented two approaches; the first approach presented an access control matrix to evaluate the risk of granting access depending on user-permission assignments. The second approach specified the best contextual role that provides the lowest risk and allows maximum accessibility by integrating security risk with RBAC.
Bijon et al. [13]	This paper proposed a framework that combines the RBAC with the security risk to specify access decisions. The paper introduced the concept of RBAC-based risk-awareness and also provided a formal description of an adaptive risk-aware RBAC model.
Dos Santos et al. [37]	This paper presented a dynamic risk-based model to achieve a highly scalable system in a cloud federation. In addition, the paper introduced a prototype implementation for the proposed model to show the effectiveness of their suggested model.
Khambhammettu et al. [6]	This paper presented a framework depending on subject trustworthiness, object sensitivity, and the difference between them using a risk assessment. However, this framework requires a system administrator with broad experience to provide a sensible metric for each input before conducting the risk assessment process.
Li et al. [24]	This paper utilized the fuzzy logic system to estimate the risk associated with access to healthcare information. Three risk factors involving action severity, data sensitivity, and risk history were utilized. In addition, a fuzzy risk metric is assigned to each risk factor to decide whether granting or denying access.
Burnett et al. [53]	This paper proposed a trust and risk-aware access control model that provides policy coverage and dynamic access decisions. The paper defined a zone policy model that allows the data owner to have total control over his/her own data. Trust is used to define the verification of whether the requester respected the obligations that are assigned to him/her or not. The paper also utilized a probabilistic computational trust model, called subjective logic, to formulate their trust assessment. The risk estimation was done using a classic method of defining expected loss in term of unwanted disclosure.
Babu and Bhanu [45]	This paper proposed building a trust and risk-based access control model to provide access decisions in cloud computing. The paper introduced a privilege management procedure that combines the security risk with trust to create an efficient and scalable access control system.
Choi et al. [23]	This paper presented a framework for a context-sensitive risk-based model for medical information systems. This framework categorized information to calculate the risk value and apply the risk through treatment-based permission profiling and specifications. This framework provided the access decision based on the severity of the context and treatment.
Namitha et al. [31]	This paper implemented a risk-based access control model based on user features including years of experience, designation, defect level, location index, time index, and probationary period and estimate the risk value using a mathematical function.
Armando et al. [56]	This paper proposed a framework that integrates the risk with trust to provide access decisions. The access decision is determined by comparing the risk value with the trust, in which the access is granted if the trust value is higher than the risk value. The paper also presented mitigation strategies to increase the trust level and reduce the risk.

Diaz-Lopez et al. [30]	This paper presented a risk-based access control model that adopted dynamic countermeasures to adjust to various changes in the risk value of system resources. The paper utilized genetic algorithms to build the most suitable set of countermeasures for a specific situation.
Dos Santos et al. [1] and Dos Santos et al. [22]	The paper [1] proposed a risk-based access control model that uses the idea of quantifying risk and aggregating them to decide access decisions. The risk value is mainly evaluated based on predetermined risk policies that are created either by the system security administrator or the resource owner. Further, a prototype of this model is created using risk metrics provided in the work of Sharma et al. [40]. This work was extended in [22] to develop an ontology-based method to estimate the risk value depending on the context and adjusting values of risk metrics and using predetermined access policies to make the access decision.
Metoui et al. [49] and Metoui et al. [52]	The paper [49] proposed a risk-aware framework that combines the privacy risk with the user trust to identify threats related to each access request. The access decision is determined by comparing the privacy-risk with the user trust in which if the user trust is higher than the privacy risk, the access will be granted. Otherwise, access will be denied. This work was extended in [52] to implement the risk estimation process based on privacy risk and user trust. In addition, several access scenarios were presented to show the effectiveness of their proposed risk estimation approach. The paper [52] also introduced adaptive adjustment strategies to increase the trust level and reduce privacy risk.
Atlam et al. [41], Atlam et al. [42] and Atlam and Wills [29]	The paper proposed [41] a dynamic and adaptive risk-based access control model by using user context, resource sensitivity, action severity, and risk history to compute the security risk value related to each access request. The paper also proposed using a smart contract to track user behavior during access sessions to detect and prevent malicious actions. This work was extended in [42] to show the validation of the proposed risk-based model using 20 security experts. In addition, the paper [42] discussed some of the risk estimation techniques and proposed the fuzzy logic system as the most appropriate approach for the IoT context where there are no available datasets. This work was extended in [29] to propose the fuzzy logic system with expert judgement as the risk estimation method to implement their proposed risk-based model. The paper showed a detailed description of using the fuzzy logic system to estimate the security risk value associated with each access request, showing the access control scenarios of the network router.
Atlam et al. [9]	The paper introduced eXtensible Access Control Markup Language (XACML) as the suitable language for implementing access control policies for the IoT system. In addition, the paper adopted XACML to build the access policies for the risk-based access control model.
Atlam et al. [43]	This paper provided an overview of risk estimation techniques in risk-based access control for the IoT. The paper discussed the benefits and drawbacks of various quantitative risk estimation techniques that are required to implement a risk-based access control model.
Dankar et al. [54]	This paper proposed a conceptual risk-aware model, which utilizes real-time and contextual information in the surrounding environment to make the access decision. The paper also implemented some mitigation measures to enforce the access decision in case of having a high-risk value in the access request.
Rahmati et al. [51]	This paper introduced a risk-based access control model to build a system called Tyche, which is a system that controls the risk in physical devices. Tyche presents the concept of risk-based access decisions in which it classifies various applications into several risk groups. Then, each risk group has a set of permissions based on the risk value.

RQ2: What are the risk factors used to build risk-based access control models?

One of the essential parts of a risk-based access control model is to choose the effective risk factors that determine access decisions efficiently. Many risk factors can be used to estimate the risk value associated with the access request to make the access decision dynamically and efficiently. To answer this research question, risk factors utilized in recent risk-based access control models were reviewed. Then, a brief overview of these risk factors is provided. This is followed by showing the risk factors extracted from retrieved/analyzed publications, as depicted in Table 5.

Table 5. Risk factors used in retrieved/analyzed publications of risk-based access control models.

Citation	Benefits of User	Action Severity	Resource Sensitivity	Outcomes of ACTIONS	Context	Trust	Risk History	Access Policies	Role
Ricardo et al. [22]	-	✓	✓	-	-	-	-	-	-
Chen et al. [4]	✓	-	-	-	-	-	-	-	-
Diep et al. [20]				✓					
Dos Santos et al. [1]	-	-	-	-	-	-	✓	-	-
Choi et al. [23]	-	-	-	-	✓	-	-	-	-
Khambhammettu et al. [6]	-	-	✓	-	-	✓	-	-	-
Li et al. [24]	-	✓	✓	-	-	-	✓	-	-
Baracaldo and Joshi [26]	-	-	-	-	-	✓	-	-	✓
Kandala et al. [27]	-	-	-	✓	✓	-	✓	✓	-
Lee et al. [28]	-	-	-	-	✓	-	-	-	-
Atlam and Wills [29]	-	✓	✓	-	✓	-	✓	-	-
Diaz-Lopez et al. [30]	-	-	-	-	-	-	✓	-	-
Shaikh et al. [5]	-	-	-	-	-	✓	✓	-	-
Wang & Jin [15]	-	-	-	✓	-	-	-	-	-
Namitha et al. [31]	-	-	-	-	✓	-	-	-	✓
McGraw et al. [32]	✓	-	-	✓	✓	-	-	✓	-
Molloy et al. [33]	-	-	-	✓	-	-	-	-	-
Ni et al. [34]	-	-	✓	-	-	-	-	-	-
Abie and Balasingham [35]	-	-	-	-	✓	-	-	-	-
Shaikh et al. [36]	-	-	✓	✓	-	✓	✓	-	✓
Dos Santos et al. [37]	-	-	-	-	-	-	-	✓	-
Molloy et al. [38]	-	-	-	✓	-	-	-	-	-
Rajbhandari and Snekkenes [39]	✓	-	-	-	-	-	-	-	-

Sharma et al. [40]	✓	✓	✓	-	-	-	-	-	-
Atlam et al. [41]	-	✓	✓	-	✓	-	✓	-	-
Atlam et al. [42]	-	✓	✓	-	✓	-	✓	-	-
Molloy et al. [44]	-	-	-	✓	-	-	✓	-	-
Babu and Bhanu [45]	-	-	-	-	-	✓	-	-	✓
Clark et al. [46]	-	-	-	✓	-	-	-	-	✓
Helil et al. [47]	-	-	-	-	-	✓	✓	-	-
Badar et al. [48]	-	-	-	-	-	-	-	-	✓
Bijon et al. [13]	✓	-	-	-	✓	-	✓	-	✓
Metoui et al. [49]	-	-	-	-	-	✓	✓	-	-
Atlam et al. [9]	-	✓	✓	-	✓	-	✓	-	-
Chun and Atluri[50]	-	-	-	-	✓	-	-	-	-
Metoui et al. [52]	-	-	-	-	-	✓	✓	-	-
Burnett et al. [53]	-	-	✓	✓	-	✓	-	-	-
Dankar et al. [54]	-	-	✓	-	✓	-	✓	-	-
Abomhara et al. [55]	-	✓	-	-	✓	-	✓	-	-
Armando et al. [56]	-	-	-	-	-	✓	✓	-	-
Chen and Crampton [57]	✓	-	-	-	-	✓	-	-	✓

- **Subject Clearance (Role)**: It represents the subject security level acquired from the system administrator. The most popular clearances in the military are Top Secret, Secret, Confidential, and no clearance. Different access permissions are granted according to the subject role in the organization. Each role is associated with certain permissions [58]. The higher the clearance granted, the lower the associated risk value.
- **Resource Sensitivity**: It describes the sensitivity level of resources the user wants to access. Different sensitivity levels have different risk values. The higher the resource sensitivity, the higher the risk value if the access is granted to this resource [24].
- **Action Severity**: It characterizes the cost of a particular action on a particular resource in terms of confidentiality, integrity, and availability. So, different actions have different consequences and so have different risk values.
- **Risk History**: It represents user previous risk values on a certain resource. It can be used to detect the future behavior of the user toward a certain resource.
- **Trust**: It is similar to the risk history. It represents the subject/user trust toward a certain resource. Trust is classified into two categories: identity and behavioral trust. Identity trust is concerned with validating the authenticity of an object and focuses on objective credentials. While behavioral trust works with the entity's trustworthiness, which depends on certain contexts [59]. In risk-based access control models, only behavioral trust is used.
- **Benefits of User**: It describes any sort of advantages/privileges the user will get when the access is granted. It also represents what will be the damage that will happen for the user if the access was denied [4].

- **Outcomes of Actions**: The access control system has inputs, consisting of the action and list of consequence outcomes of the action. Each outcome may occur in some specific contexts, consisting of principle context, environment context, and resource context. The outcome of actions estimates the risk of each of these contexts [20].
- **Context**: It signifies the real-time and environmental information that can be collected while making the access request. Contexts features are utilized to specify the security risk value related to each access request. Location and time are the most popular contexts [41].
- **Access Policies**: They are primarily utilized by the access control manager (risk estimation module in the risk-based access control model) to specify access decisions. These policies are designed by the resource owner or security system administrator to classify terms and situations of granting or denying access to a particular resource. In the risk-based control model, the estimated risk value resulted from the risk estimation module is compared against risk policies to decide whether granting or denying access [41].

The results show that risk factors used to implement risk-based access control models are significantly based on the context where the risk-based access control model will be deployed. However, several risk factors can be applied in various contexts. Reviewing risk factors used in risk-based access control models of retrieved publications reveal that "Risk History" was the dominant risk factor in most risk-based access control models in which it was adopted in 18 publications, as depicted in Figure 7. This should be normal or expected, as any risk model would or should use their previous risk values given to a user/subject to assess their current and future access. In addition, the context was one of the significant risk factors used in 14 publications. Using the context as a risk factor in risk-based access control models customizes the risk model to a specific application and adds the flexibility needed for these access control models to be able to adapt to their environment. Resource sensitivity and trust were adopted in 12 and 11 risk-based models, respectively. As a conclusion, determining the appropriate risk factors for building a risk-based access control model is significantly based on the application and environment where this model will be deployed. It also depends on the availability of data for such a risk factor to be able to use it to calculate the overall security risk value associated with the access request to determine the access decision.

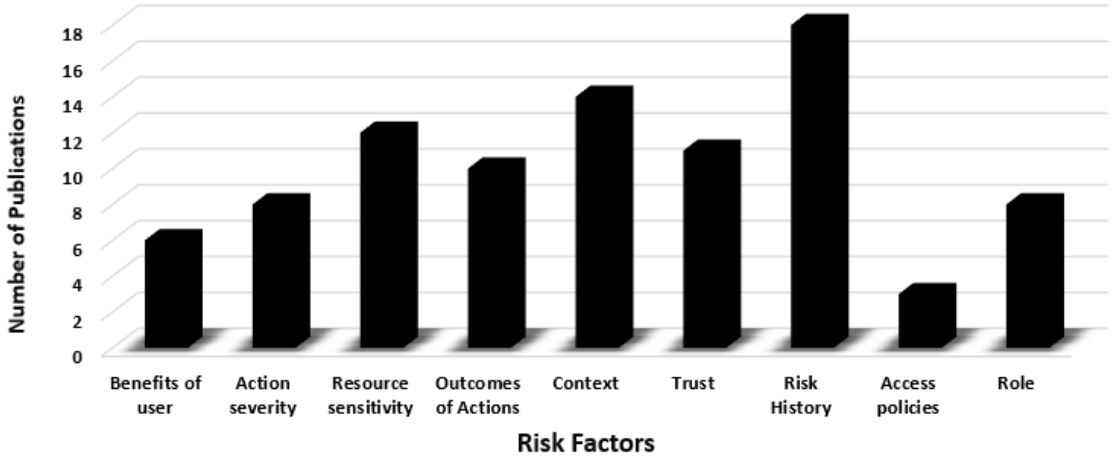

Figure 7. Risk factors used to build risk-based access control models that are discussed in retrieved publications.

RQ3: What are risk estimation techniques employed in risk-based access control models?

The vital stage of implementing a risk-based access control model is the risk estimation process. This process is based on estimating the likelihood of information leakage and the value of that information. The main purpose of the risk estimation process is to build a method to arrange risks based on their priorities and use risk values to make access decisions following a specific context.

There are several challenges associated with the risk estimation process. For example, the key purpose of the risk estimation process is to forecast the future likelihood of information leakage and the impact of such leakage on system resources. Defining such a likelihood is not an easy job [60]. Moreover, if the risk estimation process is based on imprecise or incomplete information, it will result in complications and problems to identify the value of information [31].

Determining the suitable risk estimation technique for building a risk-based access control models is not an easy task, as there are many things that should be taken into consideration: for instance, the availability of data that describe the risk likelihood and its impact. In addition, in the access control context, the security risk value will be used to determine the access decision whether granting or denying access, which requires having a precise and accurate quantitative/numeric risk value.

This section answers the third research question by investigating and reviewing various risk estimation techniques utilized in risk-based access control models of retrieved/analyzed publications, as shown in Table 6.

Table 6. Risk estimation techniques used in retrieved/analyzed publications of risk-based access control models.

Citation	Fuzzy Logic	Machine Learning	Game Theory	Risk Assessment	Mathematical Equation	Not Discussed
Chen et al. [4]	✓	-	-	-	-	-
Diep et al. [20]	-	-	-	✓	-	-
Lee et al. [28]	-	-	-	✓	-	-
Chun and Atluri [50]	-	-	-	-	-	✓
McGraw et al. [32]	-	-	-	-	-	✓
Molloy et al. [44]	-	-	-	-	✓	-
Clark et al. [46]	-	-	-	-	-	✓
Ni et al. [34]	✓	-	-	-	-	-
Helil et al. [47]	-	-	-	-	✓	-
Kandala et al. [27]	-	-	-	-	-	✓
Molloy et al. [33]	-	✓	-	-	-	-
Rajbhandari and Snekkenes [39]	-	-	✓	-	-	-
Shaikh et al. [36]	-	-	-	-	✓	-
Wang and Jin [15]	-	-	-	-	-	✓
Abie and Balasingham [35]	-	-	✓	-	-	-
Arias-Cabarcos et al. [25]	✓	-	-	-	-	-
Chen and Crampton [57]	-	-	-	-	-	✓
Molloy et al. [38]	-	✓	-	-	-	-
Shaikh et al. [5]	-	-	-	-	-	✓
Sharma et al. [40]	-	-	-	-	✓	-
Baracaldo and Joshi [26]	-	-	-	✓	-	-
Badar et al. [48]	-	-	-	-	-	✓
Bijon et al. [13]	-	-	-	-	✓	-
Dos Santos et al. [37]	-	-	-	-	-	✓
Khambhammettu et al. [6]	-	-	-	✓	-	-
Li et al. [24]	✓	-	-	-	-	-

Burnett et al. [53]	-	-	-	-	✓	-
Dos Santos et al. [1]	-	-	-	-	-	✓
Babu and Bhanu [45]	-	-	-	✓	-	-
Choi et al. [23]	-	-	-	✓	-	-
Namitha et al. [31]	-	-	-	-	✓	-
Armando et al. [56]	-	-	-	-	-	✓
Diaz-Lopez et al. [30]	-	-	-	-	-	✓
Dos Santos et al. [22]	-	-	-	-	-	✓
Metoui et al. [49]	-	-	-	-	-	✓
Atlam et al. [41]	-	-	-	-	-	✓
Atlam et al. [43]	✓	-	✓	✓	-	-
Dankar et al. [54]	-	-	-	-	✓	-
Metoui et al. [52]	-	-	-	-	-	✓
Atlam et al. [9]	-	-	-	-	-	✓
Atlam et al. [42]	✓	-	-	-	-	-
Rahmati et al. [51]	-	-	-	-	-	✓
Atlam and Wills [29]	✓	-	-	-	-	-

As discussed earlier, one of the challenges of implementing a reliable and effective risk-based access control model is to determine the risk estimation technique that produces accurate and precise risk values to determine the access decision. However, due to the unavailability of datasets that describe risk likelihood and its impact, most publications did not discuss a clear method to assess the security risks of each access request. This reflected on having 18 publications from retrieved papers without a risk estimation process.

On the other hand, there are 8 publications that proposed a mathematical equation based on relationships between input and output variables to estimate the risk. However, these mathematical equations are variable dependent and cannot be adopted in different environments. In the same way, there are 7 publications that proposed the fuzzy logic system for the risk estimation process. However, the major issue in that method is the subjectivity and the need for domain experts to define fuzzy variables and build fuzzy rules. In addition, there are 7 publications that utilized the risk assessment to determine risks and assign them priorities. However, the risk assessment itself cannot provide a numeric risk value that can be used to make the access decision. For the machine learning and game theory as risk estimation methods, there are a few publications that discussed these methods. This is due to the lack of datasets that are required for training and testing phases in machine learning and for building appropriate strategies in game theory.

As discussed, providing a dataset that describe risk likelihood and its impact on a specific context is one of the key issues of implementing risk-based access control models. We encourage various researchers to build and share different datasets regarding risk-based access control models that can improve the performance and add learning ability to current risk-based access control models. Having datasets that consider different risk factors in different domains can help researchers improve and optimize their current risk-based models. There are no specific criteria for a dataset for the risk-based access control model except it should provide quantitative values of risk likelihood and its impact for a set of access control scenarios in a specific context with the specifying risk factors adopted.

7. Conclusions

Current access control models provide a static way to provide access decisions for various applications. However, an access control model for a dynamic and distributed system should rely on contextual and real-time data. With billions of sensors and devices in our environment, contextual information can be collected and utilized in the access control process, which can provide what is called dynamic access control models. One of these dynamic models is the risk-based access control model. This model is capable of providing the access decision dynamically by estimating the security risk value associated with the access request. The risk-based access control model can provide several benefits for several trending technologies such as IoT, cloud computing, etc. This paper presented a systematic literature review and analysis of the state-of-the-art of the risk-based access control model to provide a detailed understanding of the topic. Based on the selected search strategy, 44 articles (of 1044 articles) were chosen for a closer examination in terms of recent risk-based models, risk factors, and risk estimation techniques. The results provided a summarized version of selected articles to give the reader a basic view of different risk-based access control models from the perspective of various researchers. Although there are several risk factors that can be applied in various contexts—for example, risk history, which was adopted in 18 publications—the results show that risk factors used to implement risk-based access control models are significantly based on the context/domain. In addition, the results demonstrated that providing an efficient and accurate risk estimation technique that can be applied in different domains is one of the major issues of implementing risk-based access control models. Although some risk estimation approaches can work well such as decision tree, the lack of a dataset to represent the likelihood and impact of each risk scenario in a specific context is the key problem.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest

References

1. Dos Santos, D.R.; Westphall, C.M.; Westphall, C.B. A dynamic risk-based access control architecture for cloud computing. In Proceedings of the IEEE/IFIP NOMS 2014—IEEE/IFIP Network Operation and Managment Symposioum, Krakow, Poland, 5–9 May 2014; pp. 1–9.
2. Liu, J.K.; Au, M.H.; Huang, X.; Lu, R.; Li, J. Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 484–497.
3. Suhendra, V. A Survey on Access Control Deployment. In *Communications in Computer and Information Science*; Kim, T., Adeli, H., Fang, W., Villalba, J.G., Arnett, K.P., Khan, M.K., Eds.; Springer: Berlin/Heidelberg, German, 2011; Vol. 259, pp. 11–20.
4. Chen, P.; Pankaj, C.; Karger, P.A.; Wagner, G.M.; Schuett, A. Fuzzy Multi—Level Security : An Experiment on Quantified Risk—Adaptive Access Control. In Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP'07), Ouckland, CA, USA, 20–23 May 2007; pp. 222–227.
5. Shaikh, R.A.; Adi, K.; Logrippo, L. Dynamic risk-based decision methods for access control systems. *Comput. Secur.* **2012**, *31*, 447–464.
6. Khambhammettu, H.; Boulares, S.; Adi, K.; Logrippo, L. A framework for risk assessment in access control systems. *Comput. Secur.* **2013**, *39*, 86–103.
7. Hulsebosch, R.J.; Bargh, M.S.; Lenzini, G.; Ebben, P.W.G.; Iacob, S.M. *Context Sensitive Adaptive Authentication*; Springer: Berlin/Heidelberg, Germany, 2007.
8. Houlis, P. The History and Future of Access Control Credentials 2018. Available online: https://www.ifsecglobal.com/global/history-future-access-control-credentials/ (accessed on 09 March 2019).
9. Atlam, H.F.; Alassafi, M.O.; Alenezi, A.; Walters, R.J.; Wills, G.B. XACML for Building Access Control Policies in Internet of Things. In Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018), Madeira, Portugal, 19–21 May 2018.
10. Metoui, N. Privacy-Aware Risk-Based Access Control Systems. Ph.D. Thesis, University of Trento, Trento, Italy, May 2018.

11. Bugiel, S.; Heuser, S.; Sadeghi, A.-R. Flexible and fine-grained mandatory access control on Android for diverse security and privacy policies. In Proceedings of the 22nd USENIX Security Symposium, Washington, DC, USA 14–16 Auguust 2013; pp. 131–146.
12. Hulsebosch, R.J.; Salden, A.H.; Bargh, M.S.; Ebben, P.W.G.; Reitsma, J. Context sensitive access control. In Proceedings of the Tenth ACM Symposium on Access Control Models and Technologies, Stockholm Sweden, 1–3 June 2005, pp. 111–119.
13. Bijon, K.Z.; Krishnan, R.; Sandhu, R. A framework for risk-aware role based access control. In Proceedings of the IEEE Conference on Communications and Network Security, National Harbor, MD, USA, 14–16 October 2013; pp. 462–469.
14. Kumar, A.; Karnik, N.M.; Chafle, G. Context sensitivity in role-based access control. *Oper. Syst. Rev.* **2002**, *36*, 53–66.
15. Wang, Q.; Jin, H. Quantified risk-adaptive access control for patient privacy protection in health information systems. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security—ASIACCS '11, Hong Kong, China, 22–24 March 2011; pp. 406–410.
16. Brooks, T.; Caicedo, C.; Park, J.S. Security Vulnerability Analysis in Virtualized Computing Environments. *Int. J. Intell. Comput. Res.* **2012**, *3*, 263–277.
17. Li, Y.; Sun, H.; Chen, Z.; Ren, J.; Luo, H. Using Trust and Risk in Access Control for Grid Environment. In Proceedings of the Security Technology, Hainan Island, China, 13–15 December 2008; pp. 13–16.
18. Elky, S. *An Introduction to Information System Risk Management*; Sans Institute: Bethesda, MD, USA, 2006.
19. Atlam, H.F.; Walters, R.J.; Wills, G.B. Fog computing and the internet of things: A review. *Big Data Cogn. Comput*. **2018**, *2*, 1–18.
20. Diep, N.N.; Hung, L.X.; Zhung, Y.; Lee, S.; Lee, Y.; Lee, H. Enforcing Access Control Using Risk Assessment. In Proceedings of the Fourth European Conference on Universal Multiservice Networks, Toulouse, France, 14–16 February 2007; pp. 419–424.
21. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; University of Durham: Durham, UK, 2007.
22. Ricardo, D.; Marinho, R.; Schmitt, G.R.; Westphall, C.M.; Westphall, C.B. A Framework and Risk Assessment Approaches for Risk-based Access Control in the Cloud. *J. Netw. Comput. Appl.* **2016**, *74*, 1–27.
23. Choi, D.; Kim, D.; Park, S. A Framework for Context Sensitive Risk-Based Access Control in Medical Information Systems. *Comput. Math. Methods Med.* **2015**, *2015*, 265132.
24. Li, J.; Bai, Y.; Zaman, N. A fuzzy modeling approach for risk-based access control in eHealth cloud. In Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Melbourne, Australia, 16–18 July 2013; pp. 17–23.
25. Arias-Cabarcos, P.; Rez-Mendoza, F.A.; Marín-López, A.; Díaz-Sánchez, D.; Sánchez-Guerrero, R. A metric-based approach to assess risk for 'On cloud' federated identity management. *J. Netw. Syst. Manag.* **2012**, *20*, 513–533.
26. Baracaldo, N.; Joshi, J. An adaptive risk management and access control framework to mitigate insider threats. *Comput. Secur.* **2013**, *39*, 237–254.
27. Kandala, S.; Sandhu, R.; Bhamidipati, V. An Attribute Based Framework for Risk-Adaptive Access Control Models. In Proceedings of the Sixth International Conference on Availability, Reliability and Security, Vienna, Austria, 22–26 August 2011; pp. 236–241.
28. Lee, S.; Lee, Y.W.; Diep, N.N.; Lee, S.; Lee, Y.; Lee, H. Contextual Risk-based access control. *Secur. Manag.* **2007**, *2007*, 406–412.
29. Atlam, H.F.; Wills, G.B. An efficient security risk estimation technique for Risk-based access control model for IoT. *Internet Things* **2019**, *6*, 1–20.
30. Diaz-Lopez, D.; Dolera-Tormo, G.; Gomez-Marmol, F.; Martinez-Perez, G. Dynamic counter-measures for risk-based access control systems: An evolutive approach. *Futur. Gener. Comput. Syst.* **2016**, *55*, 321–335.
31. Namitha, S.; Gopalan, S.; Sanjay, H.N.; Chandrashekaran, K. Risk Based Access Control In Cloud Computing. In Proceedings of the International Conference on Green Computing and Internet of Things (ICGCloT), Delhi, India, 8–10 October 2015; pp. 1502–1505.
32. McGraw, R. *Risk-Adaptable Access Control (RAdAC)*; National Security Agency: Fort Meade, MD, USA, 2009.
33. Molloy, I.; Dickens, L.; Morisset, C.; Cheng, P.; Lobo, J.; Russo, A. *IBM Research Report Risk-Based Access Control Decisions under Uncertainty*; IBM: Armonk, NY, USA; 2011, Volume 25121.

34. Ni, Q.; Bertino, E. Lobo, J. Risk-based access control systems built on fuzzy inferences. In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, Beijing, China, 13 April 2010; pp. 250–260.
35. Abie H.; Balasingham, I. Risk-Based Adaptive Security for Smart IoT in eHealth. In Proceedings of the 7th International Conference on Body Area Networks, Oslo, Norway, 24–26 September 2012; pp. 269–275.
36. Shaikh, R.A.; Adi, K.; Logrippo, L.; Mankovski, S. Risk-based decision method for access control systems. In Proceedings of the PST 2011: 9th International Conference on Privacy, Security and Trust, Montreal, QC, Canada, 19–21 July 2011; pp. 189–192.
37. Ricardo dos Santos, D.; Westphall, C.M.; Westphall, C.B. Risk-based Dynamic Access Control for a Highly Scalable Cloud Federation. In Proceedings of the Seventh International Conference on Emerging Security Information, Systems and Technologies (SECUREWARE 2013), Barcelona, Spain, 25–31 August 2013; pp. 8–13.
38. Molloy, I.; Dickens, L.; Lobo, J.; Morisset, C.; Russo, A. Risk-Based Security Decisions Under Uncertainty Categories and Subject Descriptors. *Data Appl. Secur. Priv.* **2012**, 157–168, doi:10.1145/2133601.2133622.
39. Rajbhandari L.; Snekkenes, E.A. Using game theory to analyze risk to privacy: An initial insight. In *Privacy and Identity Management for Life*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 41–51.
40. Sharma, M.; Bai, Y.; Chung, S.; Dai, L. Using risk in access control for cloud-assisted ehealth. 2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems, Liverpool, UK, 25–27 June 2012; pp. 1047–1052.
41. Atlam, H.F.; Alenezi, A.; Walters, R.J.; Wills, G.B.; Daniel, J. Developing an adaptive Risk-based access control model for the Internet of Things. In Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, 21–23 June 2017; pp. 655–661.
42. Atlam, H.F.; Alenezi, A.; Hussein, R.K.; Wills, G.B. Validation of an Adaptive Risk-based Access Control Model for the Internet of Things. *Int. J. Comput. Netw. Inf. Secur.* **2018**, *10*, 26–35.
43. Atlam, H.F.; Alenezi, A.; Walters, R.J.; Wills, G.B. An overview of risk estimation techniques in risk-based access control for the internet of things. In Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, Porto, Portugal, 24–26 April 2017.
44. Molloy, I.; Cheng, P.C.; Rohatgi, P. Trading in risk: Using markets to improve access control. In Proceedings of the New Security Paradigms Workshop, Oxford, UK, 8–11 September 2009; pp. 107–125.
45. Babu B.M.; Bhanu, M.S. Prevention of Insider Attacks by Integrating Behavior Analysis with Risk based Access Control Model to Protect Cloud. *Procedia Comput. Sci.* **2015**, *54*, 157–166.
46. Clark, J.A.; Tapiador, J.E.; McDermid, J.; Cheng, P.-C.; Agrawal, D.; Ivanic, N.; Slogget, D. Risk based access control with uncertain and time-dependent sensitivity. In Proceedings of the 2010 International Conference on Security and Cryptography (SECRYPT), Athens, Greece, 26–28 July 2010.
47. Helil, N.; Kim, M.; Han, S. Trust and risk based access control and access control constraints. *KSII Trans. Internet Inf. Syst.* **2011**, *5*, 2254–2271.
48. Badar, N.; Vaidya, J.; Atluri, V.; Shafiq, B. Risk based access control using classification. In *Automated Security Management*; Springer International Publishing: Cham, Switzerland, 2013; pp. 79–95.
49. Metoui, N.; Bezzi, M.; Armando, A. Trust and risk-based access control for privacy preserving threat detection systems. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer Science+Business Media: Berlin, Germany, 2016; Volume 10018 LNCS, pp. 285–304.
50. Chun, S.A.; Atluri, V. Risk-Based Access Control for Personal Data Services. In *Algorithms, Architectures and Information Systems Security*; World Scientific: Sinagapore, 2008; pp. 263–283.
51. Rahmati, A.; Fernandes, E.; Eykholt, K.; Prakash, A. Tyche: A risk-based permission model for smart homes. In Proceedings of the 2018 IEEE Cybersecurity Development Conference, SecDev 2018, Cambridge, MA, USA, 30 September–2 October 2018; pp. 29–36.
52. Metoui, N.; Bezzi, M.; Armando, A. Risk-based privacy-aware access control for threat detection systems. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer Science+Business Media: Berlin, Germany 2017; Volume 10720 LNCS, pp. 1–30.

53. Burnett, C.; Chen, L.; Edwards, P.; Norman, T.J. TRAAC: Trust and risk aware access control. In Proceedings of the 2014 Twelfth Annual International Conference on Privacy, Security and Trust, Toronto, Canada, 23–24 July 2014; pp. 371–378.
54. Dankar F.K.; Badji, R.A risk-based framework for biomedical data sharing. *J. Biomed. Inform.* **2017**, *66*, 231–240.
55. Abomhara, M.; Koien, G.; Oleschchuk, V.; Hamid, M. Towards Risk-aware Access Control Framework for Healthcare Information Sharing. In Proceedings of the 4th International Conference on Information Systems Security and Privacy, Funchal, Madeira, Portugal, 22–24 January 2018; pp. 312–321.
56. Armando, A.; Bezzi, M.; Di Cerbo, F.; Metoui, N. Balancing trust and risk in access control. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer Science+Business Media: Berlin, Germany 2015; Volume 9415, pp. 660–676.
57. Chen, L.; Crampton, J. Risk-aware role-based access control. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer Science+Business Media: Berlin, Germany, 2012; Volume 7170 LNCS, pp. 140–156.
58. Atlam, H.F.; Walters, R.J.; Wills, G.B.; Daniel, J. Fuzzy Logic with Expert Judgment to Implement an Adaptive Risk-Based Access Control Model for IoT. *Mobile Networks Applications*. **2019**, 1-13. https://doi.org/10.1007/s11036-019-01214-w
59. Luo, J.; Ni, X.; Yong, J. A trust degree based access control in grid environments. *Inf. Sci. NY* **2009**, *179*, 2618–2628.
60. Habib K.; Leister, W. Context-Aware Authentication for the Internet of Things. In Proceedings of the Eleventh International Conference on Autonomic and Autonomous Systems Fined, Rome, Italy, 24–29 May 2015; pp. 134–139.