International Journal of Computer Science, Engineering and Information Technology (IJCSEIT),
Vol.12, No.5, October 2022

IN-DEPTH ANALYSIS AND SYSTEMATIC LITERATURE REVIEW ON RISK BASED ACCESS CONTROL IN CLOUD

Sadia Hussain, M. Hasan Islam and Haider Abbas

Department of Information Security,
National University of Sciences & Technology, Pakistan

ABSTRACT

Security in Cloud is one of the most foremost and critical feature, which can ensure the confidence of the Scientific community on Cloud environment. With the dynamic and ever changing nature of the Cloud computing environment, static access control models become obsolete. Hence, dynamic access control models are required, which is still an emergent and underdeveloped domain in Cloud security. These models utilize not only access policies but also contextual and real-time information to determine the access decision. Out of these dynamic models the Risk-based Access control model, estimates the security risk value related to the access request dynamically to determine the access decision. The exclusive working pattern of this access control model makes it an excellent choice for dynamically changing environment that rules the cloud's environment. This paper provides a systematic literature appraisal and evaluation of risk-based access control models to provide a detailed understanding of the topic. The contributions of selected articles have been summarized. The security risks in cloud environment have been reviewed, taking in the account of both Cloud Service Provider and Cloud Customer perspectives. Additionally, risk factors used to build the risk-based access control model were extracted and analyzed. Finally, the risk estimation techniques used to evaluate the risks of access control operations have also been identified.

KEYWORDS

Access control; Security Risk; Risk-based access control; Risk Estimation techniques; Risk factors; Systematic review, Cloud Computing

1. INTRODUCTION

Cloud computing is a comparatively emergent but much deliberated paradigm in Information Technology that is built on distributed computing and features such as virtualization, data externalization, service-oriented architecture and low cost of computing infrastructures. The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous on-demand network access to a shared pool of configurable resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1].

Cloud computing has many benefits for users and enterprises like reducing costs, increasing flexibility, and providing easy handling. However, in addition to the advantages of cloud computing, it also provides challenges such as Security and privacy challenges, Downtime, Platform dependencies, Limited control and flexibility [2]. Although these challenges are somehow or the other interdependent on each other, but the major concern faced by cloud providers is it security and privacy. The cloud security alliance identifies security as the primary

concern hindering the wide scale acceptance of cloud computing [3]. For a cloud to be secure it needs to answer the basic information security guide lines triad of Confidentiality, Integrity and Availability, all security challenges are more or less related to this triad.

Among the various issues and challenges, security and privacy of outsourced data are to be considered primarily, as they are the two main factors of user's concerns in the cloud adoption [4]. One of the major concerns in these fields is controlling and regularizing access to the user data and resources as per the varying degrees of sensitivity. One of the primary reasons, why so many businesses and organizations are moving towards the cloud, is the ability to access data / information from literally any location in the world with an active Internet connection. Hence, the cloud's biggest vulnerability becomes clear: if the data / information can be accessed from anywhere, a hacker can access it, too. A major variance between cloud and on-premises information security is the addition of more external threats in the cloud and this needs extensive threat identification and control in place.

This is one of the main reasons why access control is such a dire necessity in the first place: it helps to lock down and protect the cloud-based infrastructure to make sure that the only people who can access your mission-critical data are the ones who actually have the right to do so. Appropriate and reliable access control mechanisms are a must to secure data in all types of service-oriented cloud models.

The objective of this research paper is to present a systematic literature review on the recently published risk-based access control models. The selected search plan organized started with 56 articles chosen for in depth analysis, which was eventually narrowed down to 18 articles. To begin with, the contributions of the selected articles were recapitulated. From the resultant articles, the risk factors were extracted and utilized to design the risk-based access control model. Additionally, in order to evaluate security risks, risk estimation techniques were classified. The contribution of this paper can be summarized as follows:-

- An in-depth review of recent research on risk-based access control models
- Identification of Security Risks posed in cloud including both Cloud Consumer (User / Customer) and Cloud Service Provider
- Identification of different kinds of Risk Factors utilized in latest risk-based access control models.
- Pointing out latest Risk Estimation techniques used in risk-based access control models.

1.1. Access Control Systems

Access control can be deliberated as one of the most crucial components in the field of information security, which warrants to determine the permission for a subject (user) to access, use or alter an object (resource). Access control systems commonly consist of the following entities [6]:-

- Object: Resource on which access is controlled e.g. Information, files, and resources etc.
- Subject: An entity capable of accessing objects. It can be the user or his/her organization or accessing terminal or even application service program.
- Access Control Policy or Rights: The way in which a subject may access an object.

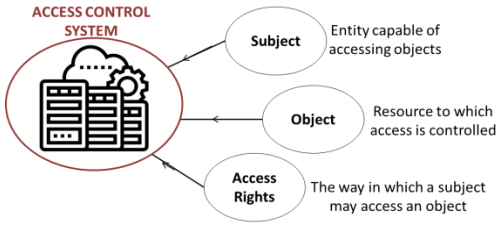

Figure 1. Components of Access Control System in Cloud

1.2. Static or Traditional Access Control Systems

There are basically two classes of Access Control Mechanisms: - (1) Static Access Control Systems and (2) Dynamic Access Control Systems. Traditional access control (also called classical or static) approaches utilize rigid, hard coded and previously defined policies to establish the access decision. These stagnant and inflexible policies result in producing the same kind of decision in entirely different situations. The commonly known traditional access control approaches include Access Control List (ACL), Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC). In an access control system, the ACL is a list of unique objects or items that involve legitimate users plus their access permissions [7]. Some of the common Static Access Control Systems in Cloud are shown in Table 1 [8-10]:-

Table 1. Features of Basic Traditional Access Control Models

SNo	Title	Model used	Features
1	Discretionary Access Control	DAC	Flexibility of information usage. Maintains the authorization database consisting of number of authorized users
2	Mandatory Access Control	MAC	Info integrity increases. Prevents the flow from low objects to high objects. Mostly used in military &govt applications. Provides multilevel security. Prevents from unauthorized users from making changes
3	Role-based access control system	RBAC model	Enhances distributed authentication services and helps to issue certificates to the Certificate Authority
4	Task Role Based Access Control	TRBAC	Associates user with permission indirectly and assigns permission according to actual needs. Permissions are activated or deactivated based on current task or process.

1.3. Dynamic Access Control Systems

As already discussed, most existing access methods are relying on manual processes and rigid policies. These approaches are unable to incorporate automation in the access control process. Whereas while making the access decision, more scalability and the ability to adjust to a variety of situations should be provisioned. Dynamic access control models not only access policies but also dynamically changing contextual features collected at the time of the access request [11]. Therefore, dynamic access control approaches should be the prerequisites for any effective and flexible access control model.

These access methods use real-time dynamic features to provide access decisions. These features include trust, context, history, risk and operational needs. Such methods can adapt to diverse

situations and environments at the time of deciding access decisions [12-13]. Security risk is one of the dynamic features that is used to build a risk-based access control model..

1.4. Risk Based Access Control Systems

Risk is the possibility of loss or a situation involving exposure to danger. It is about some incident that may arise in the future and cause losses. According to Elky [14], the risk is defined as "the possible damage that may arise from the existing operation or from some upcoming incident". In other words, Risk is the fine balance between valued danger and possible loss. Risk-based/ Risk-adaptive access control works by (1) taking into account the access parameters i.e. what a user is trying to access, how he is authenticated and also correlates with the attributes of the environment (device, servers, resources, networks etc) (2) taking into account the context of the environment / device i.e. it's history, where it has been, what it is usually accessing, from where it is accessing (geolocation), the time and date. Additionally, there is a layer of intelligence which correlates the environment properties and behavior – such as accessed websites, installed applications and more [15]. Hence, a risk adaptive access control platform will correlate all the required information and give a risk score accordingly. Based on that score it decides whether to allow, block, quarantine or limit the access to the digital asset, including database, storage, network connection, application etc.

Risk-based access control models are usually depicted by a generalized function that assigns a risk value to each request, and this function is the main difference between all such risk-based models. Risk estimation is used to determine whether an access request should be granted or denied. It takes as input several factors, including 'impact'. The out-put of this function is based on a risk threshold, and access is granted if the quantified risk for the access request is below the calculated threshold. The depiction of the generalized formula can be shown as below [16]:-

$$\text{AccessGrant}(s,o,a,c) = \begin{cases} 1 & \text{if risk } (s,o,a,c) < \text{risk Threshold otherwise } 0 \end{cases}$$

Where 's' is a subject, 'o' is an object, 'a' is an action, and 'c' represents contextual information. Hence the risk(s,o,a,c), in the equation, depicts the risk of the subject performing the action on the object, given a context. In case of result "1" represents Access Granted – "0" represents Access Denied. Since the access decisions vary according to the contextual information available at the time of request, hence, the dynamic nature of access control is captured in risk-based models. Once decision of 'Grant an Access' request has already been made, some form of monitoring after the decision is required; such as auditing, the fulfillment of obligations (conditions that must hold for a user to maintain access) or a repute system.

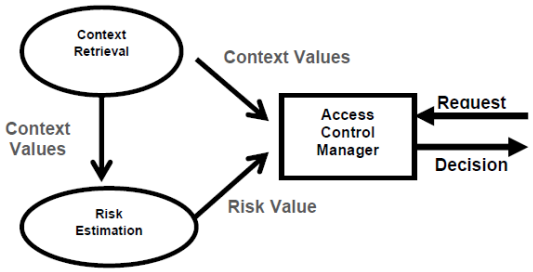

Figure 2. Overview of Risk based Access Control Model [32]

1.5. Why Select Risk Aware Access Model

Difference between Traditional Access control systems and dynamically risk aware access control systems is clearly visible in the table below:-

Table 2. Difference b/w Traditional Access Control & Risk Based Access Control

Traditional Access Control	Risk Aware Access Control
Static in nature. Depend on predefined rules that always give same result regardless of the situation	Dynamic in nature, for decisions. Dynamic features include trust, risk, context, history and operational need
Context oblivious	Flexible and context sensitive
Require a rigid authentication infrastructure. Cannot provide for distributed and dynamic environment	Use not only policies but also environment features estimated in real-time to determine access decisions
Cannot calculate risks. No capacity to adapt according to the increasing need for secure sharing.	Dynamically estimates the security risk associated with each access request to make the access decision
Assume that the risk of granting access is unacceptable if not met –no exception, protect access at all costs	Policy violations required in real applications, in unexpected situations as the policies are incomplete or conflicting. Requests may be exceptionally granted if the risk is acceptable.

2. SYSTEMATIC LITERATURE REVIEW

2.1. Methodology

The systematic literature review is a way to accumulate and inspect relevant research papers that emphasize on problems, domains, or phenomenon of similar research pattern and nature[16]. The purpose is to carry out a neutral evaluation of a research topic using arduous academic methods such as trustworthy survey methods, auditable research procedures and qualitative assessments. The SLR usually has a pre-defined research strategy, following which both supportive and unsupported research evidence is discovered and reported. The findings of this type of review can help the researcher to build foundation for supporting new research based on the discovery of gaps in the existing research status. As per guidelines proposed by Kitchenham [16], after making some revisions the systematic literature review, was carried out, which had the following repeatable steps :- (1). Ascertaining the need for systematic literature review; (2) Distinction of search strategy; (3) Selection of focal topic of study; (4) Quality assessment of the study; (5) Data extraction and monitoring; (6) Data synthesis; (7) Report result. The same are shown in the figure 3.

Figure 3. Paper Selection Process for Research Questions

2.2. Research Question Formalization

The goal of this research was to identify the most relevant access control mechanisms being used and to evaluate existing Risk Adaptive Access Control Mechanism for Critical Infrastructures in Cloud Computing Environment. This paper aims to answer the following research questions.

RQ1:	**Risk Based Access Control employs what type of solutions / techniques, in Cloud Computing environment?**
RQ2:	**Cloud Computing Environment faces what kind of probable security risks and how can they be categorized?**
RQ3:	**Risk-based access control models utilize what kind of Risk Factors?**
RQ4:	**Risk-based access control models employ what kind of Risk Estimation Techniques?**

A systematic literature review based, on the guidelines proposed by Kitchenham et al. [16], was conducted to answer the above mentioned questions. This review has focused on peer-reviewed papers that consider access control mechanisms being used and available Risk Adaptive Access Control Mechanisms in Cloud Computing Environment.

2.3. Selection Criteria

The selection criteria and procedure is used to filter out the papers that are not able to cover the research objectives or are not eligible to be surveyed. This helps to ensure the relevance of the papers selected during the principal study. Inclusion and exclusion criteria have been used for selecting the appropriate research papers, which aim to answer research questions and ensure designing of appropriate literature review. Searches were carried out via digital database libraries, out of which six computer science literature database were selected. This selection is based on the recommendation in Kitchenham's guideline. Since recent articles and papers are encouraged to be used for research, the search was confined to articles published after 2010. The search was performed in May-June, 2021 and updated in July 2022. However, the papers published after the mentioned dates are not part of this research.

The selection criteria, encompassing Inclusion Criteria, Exclusion Criteria and Database selection are shown in Table 3 [16-17].

Table 3. Selection Criteria for Choosing Relevant Papers

Criteria	Details
Inclusion Criteria	• Scientific and peer-reviewed articles • Main topic is risk-based access control model • Relevant to research questions • Articles written in English • Published after 2010
Exclusion Criteria	• 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
Database Selection	• IEEE Xplore • PubMed • Elsevier Science Direct • Google Scholar • ACM Digital Library • SpringerLink. • Grey Literature

2.4. Keyword Selection & Search Strings

To collect data from articles relevant to the specified topic and selected research questions, a search based on key-words was used. The main keywords that were emphasized are as follows:-

- Cloud Computing
- Access Control
- Risk-Based Access Control
- Security Risks
- Risk Factors
- Risk Estimation
- Risk estimation Techniques

According to the research keywords identified the following research keyword strings were utilized:

- (Access Control) AND (Cloud)
- (Security Risks) AND (Cloud Consumer) OR (Security Risks) AND (Cloud Provider)
- Risk Factors
- (Risk Estimation Techniques) AND (Cloud)
- Risk-Based Access Control

2.5. Quality Evaluation Checklist (QEC)

As discussed earlier, based on Kitchenham [16], a quality evaluation checklist has been developed to assess the different studies, in order to ensure the quality of the paper selected after inclusion and exclusion study. Each selected paper has been assessed on the basis of QEC shown in Table 4 [16-17].

Table 4. Quality Evaluation Checklist

No	Quality Evaluation Criteria	Answer	Score Ratio
1	Research questions answering the study	Yes / No / Partly	0-5
2	Scientific description of research method	Yes / No	0-5
3	Discussion of research validity threats	Yes / No	0-5
4	Discussion of contributions and limitations	Yes / No	0-5
5	Discussion of method defects	Yes / No	0-5
6	Papers published after 2016 to 2020	Yes/ No	0-5
7	No of times the paper has been cited	Number	0-5

2.6. Data Extraction and Selection

The objective of this stage is to utilize data extraction forms to record the required information researchers obtain from the primary studies. The Selection process involves the following:-

- Phase 1: Initial set of papers is retrieved after each database receives a research keyword string.
- Phase 2: Following the selection criteria and applying the research constraint; further selections are made e.g : articles' publishing year (between 2015 and 2022), content type (journal, conference paper, article), article language(English), research domain (computer science). After this the paper's abstract and introduction is reviewed. If paper meets the criteria, full text and reference are appraised. After this step, 56 articles were selected.
- Phase 3: 56 articles were carefully evaluated based on inclusion and exclusion criteria, which further resulted in the selection of 34 articles.
- Phase 4: 34 articles were gauged through the QEC. Since many articles were not able to provide any relevant information regarding our research, they were excluded. Finally, 18 articles were obtained that meet all the requirements.

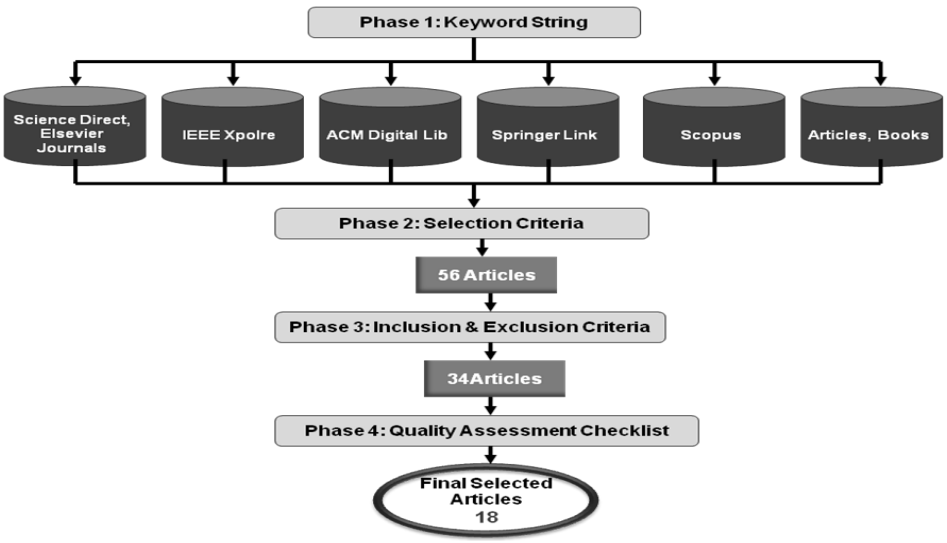

Figure 4. Paper Selection for Research Questions [17][18]

3. DATA SYNTHESIS AND DISCUSSION OF RESULTS

Finally, Data synthesis collates and summarizes the results of the included primary studies that were selected after passing through the extraction process. Synthesis can be descriptive (nonquantitative) as well as quantitative. Now we move towards our topic of interest "Risk-based access control model", which is one of the least touched but one of the most interesting topics that many researchers are exploring. In this section, a discussion on the analyzed publications is offered showing how the retrieved publications reply our proposed research questions.

3.1. RQ1: Risk Based Access Control employs what type of solutions / techniques, in Cloud Computing environment?

The retrieved publications related to risk-based access control models are being discussed to answer this research question. These selected publications are most recent and peer-review publication. Table below summarizes the contributions of each publication.

Table 5. Brief Literature Review of Risk Based Access Control Models

No	Title	Author & Year	Working Model & Advantages
1	A Framework for Context Sensitive Risk-Based Access Control in Medical Information Systems	Choi et al. [19] 2015	• Presented a framework for a context-sensitive risk-based model for medical information systems. • Categorized information to calculate the risk value and apply the risk through treatment-based permission profiling and specifications. • Provided the access decision based on the severity of the context and treatment.
2	Risk Based Access Control in Cloud Computing.	Namitha et al. [20] 2015	• Risk-based access control model based on user features including years of experience, designation, defect level, location index, time index, and probationary period • Estimate the risk value using a mathematical function.
3	Risk-aware role-based access control	Armando et al. [21] 2015	• 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. • Presented mitigation strategies to increase the trust level and reduce the risk.
4	Dynamic counter-measures for risk-based access control systems: An evolutive approach	Diaz-Lopez et al. [22] 2016	• Presented a risk-based access control model that adopted dynamic countermeasures to adjust to various changes in the risk value of system resources. • Utilized genetic algorithms to build the most suitable set of countermeasures for a specific situation.
5	A dynamic risk-based access control architecture for cloud computing	Dos Santos et al. [23] 2014	• Proposed a risk-based access control architecture for a highly scalable cloud federation. • Demonstrated the usefulness of their proposal through a prototype by using a combination of tools including XACML. • Allow resource owner to choose different risk quantification and aggregation engines through a risk policy definition file • Hosting cloud can define a baseline risk policy, to ensure that minimum security requirements are met.
6	A Framework and Risk Assessment Approaches for Risk-based Access Control in the Cloud.	Dos Santos et al. [24] 2016	• Extended model proposed by Santos (previous model) by adding three modules to the XACML 3.0 architecture(risk policy, engine & quantification) • As claimed by author, the only work that presents the idea of risk policies and to consider aspects of risk-based access control in a cloud federation
7	Trust and risk-based	Metoui et al.	• Proposed a risk-aware framework that combines the privacy

	access control for privacy preserving threat detection systems	[25] 2016 Metoui et al. [26] 2017	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.
8	A. Risk-based privacy-aware access control for threat detection systems.		• Extended model by Metoui to implement the risk estimation process based on privacy risk and user trust. • Several access scenarios were presented to show the effectiveness of their proposed risk estimation approach. • Introduced adaptive adjustment strategies to increase the trust level and reduce privacy risk.
9	Developing an adaptive Risk-based access control model for the Internet of Things.		• Proposed 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 • Proposed using a smart contract to track user behavior during access sessions to detect and prevent malicious actions.
10	Validation of an Adaptive Risk-based Access Control Model for the Internet of Things.	Atlam et al. [27] 2017 Atlam et al. [28] 2018 Atlam et al. [29] 2019	• Extended work to show the validation of the proposed risk-based model using 20 security experts • 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.
11	An efficient security risk estimation technique for Risk-based access control model for IoT.		• Further extended to propose the fuzzy logic system with expert judgement as the risk estimation method to implement their proposed risk-based model. • 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.
12	Risk Adaptive Authorization Mechanism (RAdAM) for Cloud Computing	Fall [30] 2016	• Proposed a risk adaptive authorization mechanism (RAdAM) which is a dynamic real-time risk-aware authorization mechanism for cloud computing for access decision and adaptability. • Ascertained that RAdAM follows the principles of a risk aware access control as defined in RAdAC
13	A risk-based framework for biomedical data sharing.	Dankar et al. [31] 2017	• Proposed a conceptual risk-aware model, which utilizes real-time and contextual information in the surrounding environment to make the access decision. • Implemented some mitigation measures to enforce the access decision in case of having a high-risk value in the access request.
14	An overview of risk estimation techniques in risk-based access control for the internet of things	Atlam et al. [32] 2017	• Provided an overview of risk estimation techniques in risk-based access control for the IoT. • Benefits and drawbacks of various quantitative risk estimation techniques that are required to implement a risk-based access control model were discussed.
15	XACML for Building Access Control Policies in Internet of Things.	Atlam et al. [33] 2018	• The paper introduced eXtensible Access Control Markup Language (XACML) as the suitable language for implementing access control policies for the IoT system. • Adopted XACML to build the access policies for the risk-based access control model.
16	A risk-based permission model for smart homes.	Rahmati et al. [34] 2018	• Risk-based access control model to build a system called Tyche, which controls the risk in physical devices. • Presents the concept of risk-based access decisions in which it classifies various applications into several risk groups. • Each risk group has a set of permissions based on the risk value.

17	Towards Secure Risk-Adaptable Access Control in Cloud Computing	Abdullah [35] 2018	• RAdAC model was discussed by summarizing the existing framework to formulate a strategy • Obscurity factor in protecting privacy of user was found within RAdAC framework. • Two-tier authentication scheme in RAdAC was proposed in response to security and privacy challenges through informal security analysis
18	Risk-Based Access Control Model: A Systematic Literature Review	Atlam et al. [7] 2020	• Presented the very first systematic literature review on the risk-based access control model • Compared Risk based access control models with static access control models
19	Deploying Risk Access Models in a Cloud Environment: Possibilities and Challenges	Houssein [36] 2021	• Risk-based access control models provide many security solutions to risk management in dynamic environments • Extensive investigation on access control and looked at the possibility and challenges that make a risk-based access control deployed in a cloud computing environment, successful
20	A systematic literature review for authorization and access control: definitions, strategies and models	Sayed Mohamed [37] 2022	• distinction between authorization and access control with respect to definition, strategies, and models • Compared different Access Control Models, including Risk Based Access control model and specified that this model originated from the need of real-time assessment of the current situation and possible risks even when the subjects lack proper permissions

3.2. RQ2: Cloud Computing Environment Faces What Kind of Probable Security Risks and How can They be Categorized?

The perspectives of cloud provider and cloud customer are important in this context. To answer the RQ2 five main categories of risks associated with both cloud provider and customer perspective, can be identified. Table below shows risk categories along with their subcategories. These categories include:

- Institutional or Organizational
- Technological
- Data Security and Privacy
- Physical security
- Compliance

Customers assume that once the customer organization hands over cloud computing related charge to a Cloud Service Provider (CSP), all the security automatically becomes the responsibility of the CSP. However, the customer needs to pay special emphasis on how their data is moved out from own organization towards the cloud. For this purpose risk management policies and mechanism needs to be formulated before moving towards the cloud [38]. In the table below, summary of identified risks and their mitigation is suggested through security measures. Here, CP represents cloud provider and CC represents cloud customer. Table 6: Risks and Suggested Security Measures

Table 6. Risks and Suggested Security Measures

Risk Category	Risk Sub Categories	Perspective	Security Measures
Data Security & Privacy	Ensure availability of customer's data in cloud	CP	Specific security measures have been taken by CSP to prevent outages and attacks
	Risks related to data security and privacy	CC &CP	• To mitigate these risks is using APIs to implement a robust access control, using encryption to protect data traffic. • Analyze that data is protected during design time, as during runtime. • Provide effective mechanisms for key generation, storage, and destruction of data
	Preventing unauthorized access to customer's data in the cloud	CC &CP	Can be resolved by implementing Management, authentication and authorization techniques on both customer and provider's sides
	Risks related to multi- tenancy	CP	CSP should use effective encryption methods to guarantee data isolation between clients.
	Risks related to data deletion	CP	The provider should define policies to establish procedures for the destruction of persistent media before throwing it out.
Technology	Lack of standardized technology in the cloud computing system	CC	The customer should ensure if the provider uses standardized technology and it should be mentioned in its initial contract.
	Compatibility issue between cloud and IT systems in customer's organization	CC	The solution is to use the hybrid cloud, which is capable of handling much of these compatibility issues
Organizational	Risks related to Resource Planning, Change Management	CC	Involves stakeholders in cloud adoption procedures
	Risks related security management	CC	Reevaluate existing security standards before cloud adoption.
Physical Security	The physical security of a cloud provider's data centers composed of servers, storage and network devices.	CP	Cloud providers must have certain policies and procedures in place to prevent physical security breaches these includes physical location security like alarms, CCTV cameras
Compliance	Enforce regulatory obligations in a cloud environment.	CP	• CSP must abide by all the regulations within a country, regarding cloud security. These regulations include HIPPA, FISMA • CSP has to contend with the Legal Systems under different Jurisdictions with not so much of visibility as to where the Data resides and how it is routed by passing through different Legal Jurisdictions.
	Business Continuity and Disaster Recovery	CP	Recommends replicating data across multiple infrastructures to avoid vulnerabilities in the event of a major failure

3.3. RQ3: Risk-based Access Control Models Utilize What Kind of Risk Factors?

The choice of active risk factors is one of the most crucial elements of a Risk based access control model, which help to determine access decisions in a complete manner. Multiple risk factors can be used to calculate the risk value associated with the access request effectively. For this purpose, risk factors utilized in contemporary risk-based access control models have been studied. The following risk factors have been mined and finalized after much deliberation [7], same is depicted in detail in figure 4 below:- Subject Clearance of Role

- Resource Sensitivity
- Action Severity
- Risk History Trust
- Benefits of User
- Outcomes of Actions
- Context.
- Access Policies

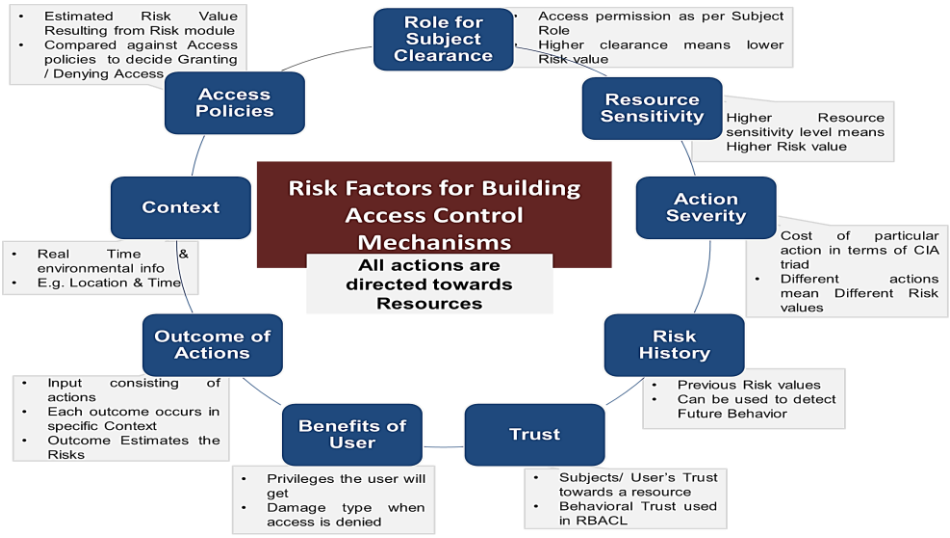

Figure 5. Active Risk Factors

The results show that in order to implement risk-based access control models, risk factors are significantly based on the context where the model needs to be deployed. However, many risk factors can be implemented in different contexts. Through different studies it was revealed that *Risk History* has been the prevailing risk factor in maximum risk-based access control models. The application and environment where the model is deployed plays a major role in determining the appropriate risk factors for building a risk-based access control model. The availability of data for a risk factor, for calculating the overall security risk value associated with the access request that determines the access decision, is also important.

3.4. RQ4: Risk-based Access Control Models Employ what Kind of Risk Estimation Techniques?

Risk estimation process is the fundamental stage in implementing a risk-based access control model. Here the likelihood of information leakage and the value of that information is assessed. The main purpose is to build a process that arranges risks based on their priorities and uses risk values to make access decisions. This is done in relation with a specific context

There are many considerations to be kept in mind while determining the suitable risk estimation techniques for constructing a risk-based access control (1) the availability of data that describe the risk likelihood and its impact (2) In access control context, the access decision whether granting or denying access, is determined by the security risk value (precise and accurate quantitative/numeric risk value).

This section examines various risk estimation techniques in order to answer RQ4, as shown in Table 7.

Table 7. Risk Estimation Techniques [32]

No	Technique	Details	Issues
1	Mathematical Equation	Mathematical equation based on relationships between input and output variables are used to estimate the risk.	• They are variable dependent • Cannot be adopted in different environments.
2	Fuzzy Logic System	• Set of mathematical rules for representing the knowledge that is based on degrees of membership. • Ensures that human common sense, intuition, and experiences are not neglected [43]	The subjectivity and the need for domain experts to define fuzzy variables and build fuzzy rules.
3	Risk Assessment	• Is used to define the extent of the potential threat and the risk associated with an IT system. • The goal is to determine the risk context and acceptability that can be done by comparison to similar risks. The type of risk analysis should be appropriate for the available data and severity of potential loss.	Risk assessment itself cannot provide a numeric risk value that can be used to make the access decision.
4	Game Theory	• Game theory consists of four elements: o Players - the strategic decision makers o Strategies - the plan o payoffs - of a given player is affected by both the actions performed by him and the other player o the information • Risk analysis can be based on priority or values related to benefit which users can provide rather than the probability. • Can be used in situations where no actuarial data is available.	• Few publications • This is due to the lack of for building appropriate strategies in game theory.
5	Machine Learning	ML is the logical examination of calculations and measurable models that computer systems use to implement a specific endeavour without using express headings, contingent upon models, and acceptance. It is a subset of computerized reasoning [40]. Types of ML algorithms include Supervised Learning (including its sub types), Unsupervised Learning (including its sub types), Semi-supervised Learning and Reinforcement Learning.	• Few publications • Lack of datasets required for training and testing phases
6	Decision Tree	• Model used to simplify decision making based on a set of rules presented as a tree. • Uses the attributes of objects for classification and decision.	• A small change in the value of an attribute could lead to a different conclusion • When scale becomes large, its difficult to understand and more data will be needed to identify and validate the rules
7	Monte Carlo Simulation	the system random behaviour is represented by performing a set of experiments on the system in the form of simulations	requires high computing power
8	Expert Judgement	risk-based decision making processes that rely significantly on a quantitative risk assessment that requires numerical data describing the event frequencies and conditional probabilities in the risk model	Dependent on Experts that should be selected from diverse fields to provide different points of views

Significant issues of implementing risk-based access control models include a. Providing a dataset to define likelihood of probable risk. b. Impact of that risk on a specific context. Different and new datasets regarding risk-based access control models will help in improving the performance and will add learning ability to current risk-based access control models. Different risk factors in different domains can help researchers to augment and fine tune their current risk-based models. Datasets 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 implemented; hence there are no specific standards for defining these datasets.

4. PROPOSED MODEL

4.1. Work Flow Mechanism

The proposed system is placed as a module between the organization's cloud and its users. In order to access any resources that are on the cloud, a user must first access the module. After login authentication, the user will get access to the interface of the module. The module then carries out access computations and if grants the user access to the resource. At the termination of access permission, the user is logged out. In addition to the abovementioned module, there is a parallel admin console and its duty is to monitor users.

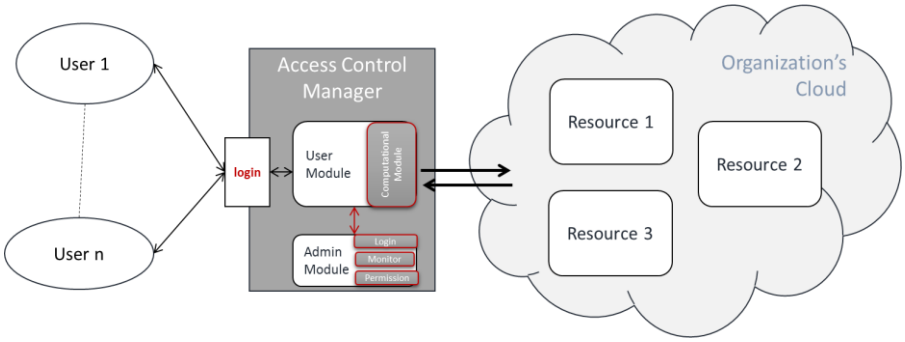

Figure 6. Block Diagram of Proposed Model

The system consists of two parts, the user console and the admin console that monitors it [39]. The user console is where the user logs in and is authenticated and the request is sent to the server. After a user has successfully logged in, they are presented with some options which are explained in section 4.2. The user chooses the files and the permissions he wants to request on those files, after which the system calculates risk values. The results of the calculation determine whether or not the user will be provided with a session. The session is when the user can access the requested files with the requested privileges on the cloud and it can be either monitored or not based on the methodology of access control that was selected. After each session terminates, a log of the user's activity is maintained. Parameters relevant to monitoring user activity are present at the admin console. The admin console can terminate a session, disable a user's account and generally monitor user activity on cloud. Following is the step-bystep breakdown of how the proposed module works:-

- **Registration and Login**. All new users have to register using their name, designation, employee ID, email ID, date of birth, and contact number. The information is saved in the database and the user is given a unique password and username. The module has to be installed on every user's machine. When a user logs in, the module checks if it is installed at the machine or not.

- **Session Grant Computations**. After the user logs in and requests to access some resource on the cloud, the module has to decide whether or not the permission should be granted. To make this decision the module performs computations that include analysis of risk parameters. The risk values considered are called Current Risk Values and Threshold Risk Values. The file permissions dictate The Current Values while risk parameters determine The Threshold Values. Prior to a session, the Current Value is calculated and compared with the Threshold Value. If Current Value <= Threshold Value then the session is granted. After the decision about the session grant is finalized as positive, a session key is created. User is given following options: i) Create a new file ii)Select an existing file & view relevant permissions.
- **Permission Grant**. When user selects permission to request, system calculates the risk associated & compares it to Threshold Value already associated with that particular user. If it is equal to or less than Threshold Value then session is granted otherwise request is denied.
- **Termination of Session**. Once the session starts, the user can access the resources on the cloud. In most cases, the session is monitored and if the user does anything that is risky, the session can be terminated. If a user's session is terminated or their account is disabled they can contact the network administrator. They will have to present justifications for their activity and prove that it was not malicious.

4.2. Computations

The previous section mentions risk parameters, the Current Value, and the Threshold Value. This section deals with how all of the values are calculated.

4.2.1. Risk Parameters.

A total of eight parameters are used to compute the final risk value.

Table 8. Parameters to Compute Final Risk

Risk Value	Minimum	Maximum
Years of Experience	0.1	0.7
Appraisal Factor	0	1
Designation	0.1	0.7
Defect Level	0.1	1
Probationary Period	1	12
Referral Index	0	1
Location Index	0	1
Time Index	0	1

Following is the detail for each parameter:-

4.2.1.1. Years of Experience

Seven different ranges for risk values relevant to years of experience, were considered.

Table 9. Risk Value as per years of Experience

Years of Experience	Risk Value
1	0.7
2	0.6
3	0.5
4	0.4
5-10	0.3
10-15	0.2
15	0.1

As seen in the table, the higher the years of experience, the less is the risk level. So a person who has been in the organization for a long time is more trustworthy than a person who has only been employed for 1 year. A person with low-risk value will get more permissions than a person with high-risk value.

4.2.1.2. Appraisal Factor

This is a value assigned by the supervisor to each employee based on sincerity. It can range from 0, 0.1...1

4.2.1.3. Designation

The designation is also a factor in trustworthiness. Generally, people at higher posts are trusted more than their junior counterparts. This is why a smaller risk value is assigned to the most senior management.

Table 10. Risk Value as per Designation

Designation	Risk Value
Highest post	0.1
	0.2
	0.3
	0.4
	0.5
	0.6
	0.7
Lowest post	0.8

4.2.1.4. Defect Level

Defect level is defined as the rate at which a particular user's activity failed during their sessions. A high defect level means the employee is less trustworthy.

Defect level = No. of sessions with fault / No of user's total sessions

4.2.1.5. Probationary Period.

Amount of time left until a new employee has completed the probation period.

4.2.1.6. Referral Index.

Referral Index bases trust on how many people vouch for a certain person. If a lot of senior people refer a junior, his risk index will be small. The scale ranges from 0.1 to 0.8

Table 11. Risk Value as per Referral Index

Referral Index	Risk Value
1	0.1
2	0.2
3	0.3
4	0.4
5	0.5
6	0.6
7	0.7
8	0.8

4.2.1.7. Location Index.

This index is the ratio of the times an employee has accessed resources from a location outside the company office and the number of times access was from the office. A high value of location index means more risk.

4.2.1.8. Time Index.

This index is the ratio of times access was during business hours verses when it was after hours. Risk is considered low when most of the access is limited to office hours.

4.2.2. Threshold Value.

The formula for Threshold Value uses all the above mentioned parameters.

Threshold Value=(§ * designation risk * referral index) /(years of experience risk * T) Where
§=Defect level
T = Time left in probation period

4.2.3. Current Value.

Can be given as the following:-

Current Value = (Defect Level + Location Index + Time Index + Appraisal Index) / 4

4.3. Summing Up.

This model uses different kinds of risk levels associated with environmental conditions for giving access decisions. However, it is difficult to be deployed because of the amount of analysis required and is currently under study for refinement.

5. CONCLUSION

Access decisions are dynamically provided by estimating the security risk value, associated with the access request, in Risk based Access Control models. Risk-based access control model can

prove beneficial in regards to several trending technologies including the cloud computing and IoT etc, despite the fact that it is one of the very less explored technique for Access Control in the Cloud environment.

The important objectives of the Systematic Literature Review presented in this paper was the identification of key questions for formulating a comprehensive study on the very less visited topic of Risk based Access Control Systems in Cloud Computing environment. This included the review of current techniques being used for Risk Based Access Control in Cloud. This paper presented an indepth analysis and systematic literature review of the current risk-based access control models to provide a detailed understanding of the topic. The analysis included both service provider and consumer in cloud computing. An important aspect reviewed was the study of Risk Factors that are building blocks of risk-based access control models. Another aspect which is selecting the appropriate risk estimation technique, especially in the cloud environment, is quite a bit of difficult task. An overview of different risk estimation techniques, that are used in existing risk-based access control models, has been discussed in this paper. Also, some of the requirements for selecting the appropriate risk estimation technique have been inspected. Machine Learning has been targeted as the possible solution for amicably solving risk based access control issues faced in the cloud environment.

6. RESEARCH CHALLENGES & FUTURE DIRECTIONS

The amount of studies and data available for current researches are not enough to facilitate in the clear understanding of Risk based access control in cloud. This indepth analysis and proposed framework contributes to organize the available knowledge and indicates future research directions. The review and analysis of the selected studies identify a number of challenges showing that there are still colossal prospects for researchers to contribute in this area. Some aspects have been generally studied such as risk estimation techniques and risk factors however topics such as threat modeling have not been touched in most of the studies till now. Challenges in this domain are therefore manifold due to the absence of practical implementation employing all the aspects in realtime.

Most of the undertaken efforts are in an early stage and many open challenges remain to be solved to successfully deploy Risk based access control in dynamically changing environments such as Health care and Disaster Management. No work has yet been done in the field of Military based environment with restrictive policies as well as educational sectors; where this type of access control can prove to be a very useful entity in controlling access. Future directions can also include the adaptability of risk based access systems in Fog Computing. Fog is useful for handling colossal volumes of data and acts as a bridge between the cloud and IoT, further offering a platform for various real-time applications and services. Another prospect is the conception of an effective and precise risk estimation technique for risk-based access control models, which is becoming an important facet in the online business sector. The absence of a dataset representing the likelihood and impact of each risk scenario in a specific context, needs to be handled affably. Empirical comparison of these risk estimation techniques can be a significant research direction. Additionally, future research can focus on how machine learning can help in proposing a viable solution to risk based access control issues.

7. LIMITATIONS OF THE REVIEW

Although the goal of this analysis was to include a diverse number of sources, however, it is impossible to evaluate all the literature available. In order to select the suitable and applicable literature several criteria were established, which may have resulted in the unintentional exclusion

of some relevant literature. This review could serve as theoretical foundation for future research, highlighting the current major security issues and their solutions. In future practical case studies in the same field can be further examined in order to validate these solutions, especially in the field of medicine and academia.

ACKNOWLEDGEMENTS

The author would like to thank everyone who has had a positive impact on her and everyone's lives, just everyone!

REFERENCES

[1] Mell, P. and Grance, T.: The NIST definition of cloud computing (2011).
[2] GözdeKarataş and AkhanAkbulut, Survey on Access Control Mechanisms in Cloud Computing, Journal of Cyber Security and Mobility, Vol: 7 Issue: 3, Published In: July 2018, doi: https://doi.org/10.13052/jcsm2245-1439.731.
[3] Mayank Raj, Mario Di Franscesco , Sajal K. Das,Secure Mobile Cloud Computing, in Handbook on Securing Cyber-Physical Critical Infrastructure, 2012.
[4] Clavister. Security in the Cloud. 2009. http://www.itwire.nu/members/cla69/attachments/CLA_WP_SECURITY_IN_THE_CLOUD.pdf.
[5] Data Security and Privacy Protection Issues in Cloud Computing, Deyan Chen, Hong Zhao, Published in International Conference on Computer Science and Electronics Engineering, 2012, DOI:10.1109/ICCSEE.2012.193
[6] R. S. Sandhu and P. Samarati, "Access control: principle and practice," Communications Magazine, IEEE, vol. 32, no. 9, pp. 40–48, 1994.
[7] Hany F. Atlam , Muhammad Ajmal Azad , Madini O. Alassafi , Abdulrahman A. Alshdadi and Ahmed Alenezi, Risk-Based Access Control Model: A Systematic Literature Review, Future Internet 2020, 12, 103; doi:10.3390/fi12060103 www.mdpi.com/journal/futureinternet
[8] Ferraiolo, D., Kuhn, R.: Role-based access controls. In: Proceedings of the 15th NIST-NCSC National Computer Security Conference, Baltimore, pp. 554–563 (1992)
[9] Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E.: Role-based access control models. IEEE Comput. 29(2), 38–47 (1996). doi:10.1109/2.485845
[10] Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D.R., Chandramouli, R.: Proposed NIST standard for role-based access control. ACM Trans. Inf. Syst. Secur. 4(3), 224–274 (2001). doi:10.1145/501978.501980
[11] 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.
[12] Shaikh, R.A.; Adi, K.; Logrippo, L. Dynamic risk-based decision methods for access control systems. Comput. Secur. 2012, 31, 447–464. [CrossRef]
[13] 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.
[14] Elky, S. An Introduction to Information System Risk Management; Sans Institute: Bethesda, MD, USA, 2006.
[15] A Framework and Risk Assessment Approaches for Risk-based Access Control in the Cloud, Daniel Ricardo dos Santos, Roberto Marinho, Gustavo Roecker Schmitt, Carla MerkleWestphall, Carlos Becker Westphall, Preprint submitted to Journal of Network and Computer Applications, July 11, 2016
[16] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering–a systematic literature review," Information and software technology, vol. 51, no. 1, pp. 7– 15, 2009.
[17] User Behavior Trust Based Cloud Computing Access Control Model; Qin Jiangcheng

[18] Rabia Latif & Haider Abbas & Saïd Assar, Distributed Denial of Service (DDoS) Attack in Cloud-Assisted Wireless Body Area Networks: A Systematic Literature Review, J Med Syst (2014) 38:128 DOI 10.1007/s10916-014-0128-8.

[19] 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. [CrossRef] [PubMed]

[20] 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.

[21] Armando, A.;Bezzi, M.;DiCerbo, F.;Metoui, N. Balancing trust and risk in access control. In Lecture Notes in Computer Science(Including Sub series Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer Science+Business Media: Berlin, Germany, 2015; Volume 9415, pp. 660–676.

[22] Diaz-Lopez, D.; Dolera-Tormo, G.; Gomez-Marmol, F.; Martinez-Perez, G. Dynamic countermeasures for risk-based access control systems: An evolutive approach. Futur. Gener. Comput. Syst. 2016, 55, 321–335. [CrossRef]

[23] 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 ManagmentSymposioum, Krakow, Poland, 5–9 May 2014; pp. 1–9.

[24] 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

[25] Metoui, N.;Bezzi, M.;Armando, A. Trust and risk-based access control for privacy preserving threatdetection 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

[26] 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.

[27] Atlam, H.F.; Alenezi, A.; Walters, R.J.; Wills, G.B.; Daniel, J. Developing an adaptive Riskbased 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.

[28] 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. [CrossRef]

[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. [CrossRef]

[30] Risk Adaptive Authorization Mechanism (RAdAM) for Cloud Computing, Doudou Fall, Takeshi Okuda, YoukiKadobayashi, Suguru Yamaguchi, Journal of Information Processing Vol.24 No.2 371–380 (Mar. 2016), [DOI: 10.2197/ipsjjip.24.371]

[31] Dankar, F.K.; Badji, R. A risk-based framework for biomedical data sharing. J. Biomed. Inform. 2017, 66, 231–240. [CrossRef]

[32] 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.

[33] Atlam,H.F.;Alassafi,M.O.;Alenezi,A.;Walters,R.J.;Wills,G.B.XACMLforBuildingAccessContro lPolicies 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.

[34] 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.

[35] Towards Secure Risk-Adaptable Access Control in Cloud Computing; Salasiah Abdullah, KhairulAzmi Abu Bakar; 2018

[36] Redia Houssein; Younis A. Younis, Deploying Risk Access Models in a Cloud Environment: Possibilities and Challenges, 2021 IEEE 1st International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering MI-STA,**IEEE Xplore:** 29 June 2021

[37] Aya Khaled Youssef Sayed Mohamed, Dagmar Auer, Daniel Hofer, Josef Küng, A systematic literature review for authorization and access control: definitions, strategies and models, International Journal of Web Information Systems, Emerald Publishing Limited 1744-0084 DOI 10.1108/IJWIS-04-2022-0077, 6 July 2022

[38] Cloud computing risk assessment: a systematic literature review Rabia Latif, Haider Abbas, Saïd Assar, Qasim Ali; HAL Id: hal-02397600 https://hal.archives-ouvertes.fr/hal-02397600 Submitted on 6 Dec 2019

[39] Sandhu, R., Coyne, E., Feinstein, H., Youman, C"Role-based access control models" IEEE Computer, Volume29, Number 2, February 1996.

[40] Molloy, I., Dickens, L., Morisset, C., Cheng, P.-C., Lobo, J.,Russo, "A Risk-based security decisions under uncertainty" In:CODASPY 2012.

[41] Salim, Farzad, Reid, Jason F., Dulleck, Uwe, & Dawson, Edward "An approach to access control underuncertainty". In ARES, IEEE, Vienna University of Technology, Vienna, pp. 1-8. In 20 11

[42] Liu, Q.; Li, Pi.; Zhao, W.; Cai, W.; Yu, S.; Leung, V.C. Asurvey on security threats and defensive techniques of machine learning. A data driven view. IEEE Access 2018, 6, 1210312117.

[43] A. Amini, Norziana Jamil, Abdul Rahim Ahmad, Hidayah Sulaiman, , A Fuzzy Logic Based Risk Assessment Approach for Evaluating and Prioritizing Risks in Cloud Computing Environment, Conference: International Conference of Reliable Information and Communication Technology, DOI:10.1007/978-3-319-59427-9_67, May 2018

[44] Shiyu Xiao,1Yuhang Ye,1Nadia Kanwal,2Thomas Newe,3and Brian Lee, SoK: Context and Risk Aware Access Control for Zero Trust System, Hindawi Security and Communication Networks Journal June 2022, Volume 2022 | Article ID 7026779 |https://doi.org/10.1155/2022/7026779

[45] Demystifying the Risk-Based Approach to Cloud Computing, metricstream: thrive on risk,https://www.metricstream.com/insights/risk-based-approach-to-cloud-computing.htm

[46] S. R. Ronald, *Risk Management Framework for Information Systems and Organizations:: A System Life Cycle Approach for Security and Privacy*, National Institute of Standards and Technology, Gaithersburg, MD, 2018.

[47] Hany F. Atlam & Gary B. Wills, ANFIS for risk estimation in risk-based access control model for smart homes, Multimedia Tools and Applications, Springer Link, Published: 04 October 2022

AUTHORS

Sadia Hussain is a student of Phd in Information Security at National University of Sciences & Technology, Pakistan. She balances her research, job and family life amicably.

Dr Hasan Islam is research scholar & teacher who has vast experience in the field of Information Security since in the last 20 years.