School of Computer Sciences, USM, Penang

CAT301 Research Methods & Special Topic Study
Semester 1, 2020/2021

Title: A Zero-Trust Access Control Model in comparison with Other Models in Cloud Hosting

Supervisor: Ts. Dr. Mohd. Najwadi Yusoff

Group Members

Name	Matric Number
1. Teh Zhen Rong	143955
2. Muhammad Iqrar Amin	140659
3. Harold Bong Jing Choy	140765

Division of Tasks

Teh Zhen Rong	Role: • *Coordinate the member in writing the paper.* • *Helping members in writing the paper.*
Muhammad Iqrar Amin	Role: • *Gather results and analyse the result.* • *Check for grammar of the paper.*
Harold Bong Jing Choy	Role: • *Gather articles and papers related to the topic.* • *Review the articles and papers.*

DECLARATION

1. This is to declare that this work under the supervision of Ts. Dr. Mohd. Najwadi Yusoff having title "A Zero-Trust Access Control Model in comparison with Other Models in Cloud Hosting" carried out in partial fulfilment of the requirements of CAT301 Research Methods and Special Topic Study is the sole property of the Universiti Sains Malaysia and the respective supervisor and is protected under the intellectual property right laws and conventions. It can only be considered/used for purposes like extension for further enhancement, product development, adoption for commercial/organizational usage, etc., with the permission of the University and respective supervisor.

This is to declare that the above publication is the sole contribution of the author(s) and no part hereof has been reproduced illegally (cut and paste) which can be considered as plagiarism. All referenced parts have been used to argue the idea and have been cited properly. We will be responsible and liable for any consequence if violation of this declaration is proven.

Teh

………………………………………

Name: Teh Zhen Rong

Matric Number: 143955

………………………………………

Name: Harold Bong Jing Choy

Matric Number: 140765

………………………………………

Name: Muhammad Iqrar Amin

Matric Number: 140659

A Zero-Trust Access Control Model in comparison with Other Models in Cloud Hosting

Teh Zhen Rong
School of Computer Science
Universiti Sains Malaysia
Gelugor, Malaysia
zhenrong1999@student.usm.my

Muhammad Iqrar Amin
School of Computer Science
Universiti Sains Malaysia
Gelugor, Malaysia
iqraramin@student.usm.my

Harold Bong Jing Choy
School of Computer Science
Universiti Sains Malaysia
Gelugor, Malaysia
haroldbongjingchoy@student.usm.my

Ts. Dr. Mohd. Najwadi Yusoff
School of Computer Science
Universiti Sains Malaysia
Gelugor, Malaysia
najwadi@usm.my

***Abstract*—Access control model one of the keys to restrict users from doing stuff that they are not permitted especially in the era of cloud computing. This paper aims to compare and find the best access control model for cloud. We had gone through papers of access control models and piece together the full picture of a model from the security stands point. NIST give us the guideline to look for into the model. The result we get is on zero-trust access control model where it scores almost all the criteria we gave. The model has the highest permission restriction and policy restriction due to the nature of it not trusting any devices and network at the first place. The next is role-based access control where the model score well in flexibility in configuration. Hence, we suggest that zero-trust access control to be used in cloud and further research is required into it.**

Keywords—Access Control Model, Security, Cloud computing, Zero-trust Access Control Model

I. Introduction

Recently, cloud computing is becoming an important platform in the modern society. It plays a vital role in enabling organizations and companies to deploy their web services without having the need to keep and service their in-house servers. Such criterion makes this operation financially sustainable overall. The lambently debated security concerns on cloud computing has empower my team to explore current cloud securities mitigations deployed by leading companies in this field.

The core of all cloud is security model which decide the allocation of services and handling traffic. There is severe security model has been proposed and used by the tech companies like Attribute Based Access Control (ABAC), Role Based Access Control (RBAC), Mandatory Access Control (MAC).

The study proposes a better security model to be implemented on the cloud. The scope of the study is in investigating the security model on cloud.

A. Background of the Problem

The cloud is cluster of computers connected to form a platform for other to use as platform for hosting. Cloud has allowed more user to use the cloud for more application and services that are unimaginable for the past and cost less. Security is the key factor that allow users host them valuable data and application on cloud to form a platform for other to use as platform for hosting. Hence, their data and application will not be leaked out or taken down by others easily. Recent studies [1] [2]has found more concern on security model than. As said in [3], finding a right cloud provider is one of the considerations in hosting on cloud. A cloud vendor affects the cloud security if the vendor does not check their security update on their hardware and software used for supplying cloud. The security model plays a key role of securing the data and help the user to manage their services they used is secure. Moreover, a good model saves a day for a user that did not implement their service focus on security.

Access Control [2] is present in cloud platform to help owner of the project to control users accessing the project created. Various model has proposed even before cloud to restrict user from doing things that are not allowed in a system [1]. This restriction also applies to program that is executing. Accessing the project become more difficult for others access the data. Hence, finding a best model for access control is important for cloud to take control of the user accessibility to cloud.

B. Objective

The main goal of this research is to study the issues related to the existing access control models and suggest a new model for cloud computing platforms. The goals of this research are:

- To survey several access control models being used in cloud hosting platforms.
- To compare Zero Trust Access Control Model among other access control models being used in cloud hosting platforms based on NIST Metric.

II. Related Work

This section discussed about three preferable access controls mechanisms in the cloud computing field today: Role-Based Access Control (RBAC), Attribute Based Access Control (ABAC) and Mandatory Access Control (MAC).

A. Role-Based Access Control (RBAC)

Role-Based Access Control was first introduced by Ferraiolo and Kuhn in 1992 with a role as the main factor in access control mechanism [3], this is then improved together with Sandhu and being published under NIST access control standards. [4] After that, the two authors work with Chandramouli and release a newer and revised version of book in Role-Based Control. [5]Role-Based access control uses users, roles, and permission to manage the access authority mode of the internal personnel of the organization. With the rules and security policies, permission will be assigned by organization to the defined role, and then the role is assigned to the user, instead of the traditional subject and recipient Authorization Mode [5], when the user is authenticated and obtains an appropriate role, he can have the permissions that the role can execute. In addition, this section will introduce the role-based access control core elements and issues.

1) RBAC Model

In RBAC, the end users are being assigned to their respective roles while their permissions are determined by their roles. There are five core elements in RBAC: users, roles, permissions, where the permissions are further extended with operations and objects, the definitions are as below [5]:

1. User: Human or programs that interact with the system.
2. Role: Usually will be the position in an organization and given appropriate permissions.
3. Permission: The authorizations towards objects, for example properties editing, save delete function etc.
4. Operation: The process activated by user to carry out certain tasks.
5. Object: Resources accessible by system such as files and peripherals.

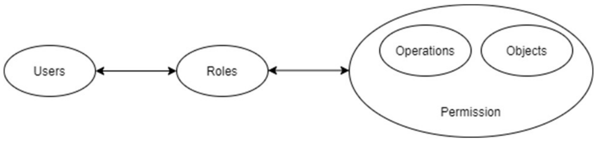

Figure II.1: RBAC Core Elements

B. *Attribute Based Access Control (ABAC)*

As of now the model definition of ABAC has not formed a unified opinion, but its central concept is clear, i.e., the characteristics of related entities (subject, object, and environment) can be used as the basis for authorization to study how access control can be conducted. The attributes of an entity can be split into subject attributes, object attributes, and environment attributes for this purpose. [6]

1) ABAC Model

Access within ABAC is based on a collection of user attributes. It can also be designated as an access control based on authentication. It extends RBAC based on the delegation of attribute authority, decentralization of attributes and interference of attributes. [2] Different from RBAC, ABAC has no need of roles as middleman, but instead describe the authority relationship directly through the strategy and leads to higher flexibility and efficiency.

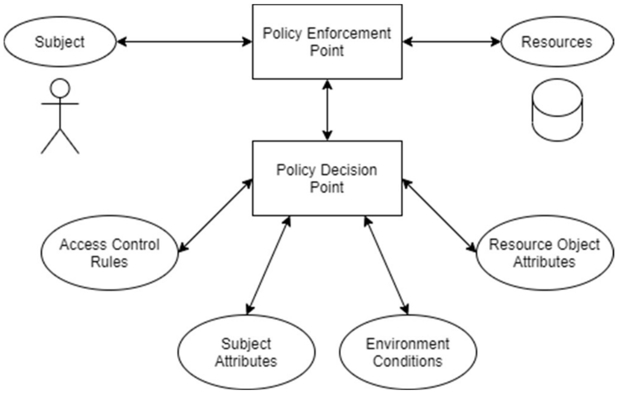

Figure II.2: ABAC Structure

C. *Mandatory Access Control (MAC)*

Mandatory Access Control (MAC) is introduced on the basis on active access control. MAC increases the security of network resources by division of attribute levels, access rights of each attribute levels are controlled by access control mandatory rules of the system to prevent intentionally or accidentally use the right of discretionary access. In the control rules of MAC, the main key rule is to not read upwards and write downwards, which means the data and information can only be passed from a low security level to a higher security level. [2] Once there is violation of data flow, the system will automatically prohibit the flow and halt down the process.

1) MAC Model

The level of security is hierarchical, with the topmost as the highest security level. In the example below are Alice and Bob in their respective security level based on the mandatory access control rules. User Alice has permission to access the resources that is classified as confidential but cannot access Bob's data as Bob is connected to the top security level.

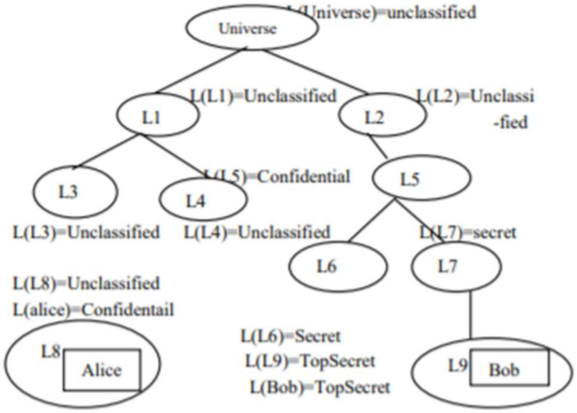

Figure II.3: Example of MAC Model [2]

D. *Zero-Trust Access Control Model (ZTAC)*

Zero-Trust Access Control (ZTAC) is introduced along with Zero-Trust architecture where the network is treated as untrusted in the first place [7]. Hence, more restriction can be added into the model using stronger authentication and authorization standards based on user- and device-specific attributes [7]. ZTAC is used in Department of Defence of United State, Google, Azure and Amazon.

1) ZTAC model

There are 6 fundamental elements [8] in ZTAC which are identities, devices, applications, data, infrastructure, and networks. The explanations of the 6 fundamental elements are listed below:

1. Identities – represent users, services or IoT devices. Verify that identity with strong authentication and the right permission.
2. Devices – platform or devices that users or services on to. Monitor and enforce device health and security.
3. Applications – application and API that has appropriate in-app permission and valid security configuration.
4. Data – is classified, labelled, and encrypted and access restricted. It is remained as safe as possible when it is transferred.
5. Infrastructure – can be on-premises server, cloud-based VMs. Containers, or micro-services. Infrastructure represents a critical threat vector.
6. Networks – should have end-to-end encryption, monitoring and analytics.

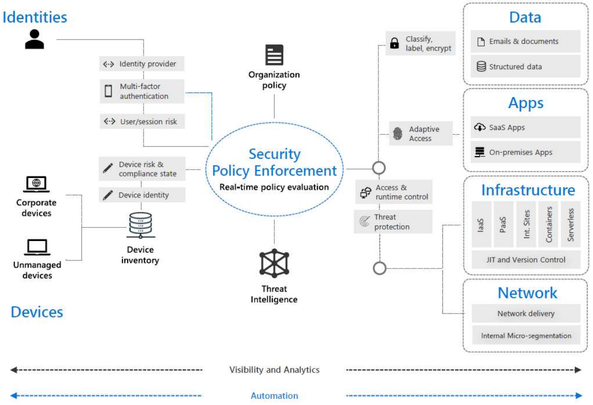

Figure II.4: Example of ZTAC Model [8]

III. Methodology

In this research we have adopted a mixed research method named Exploratory Sequential Designed Method, proposed by Lesly A. Dossett et al. [9]. The detailed description about the methodology used for evaluation is provided below.

A. *Exploratory Sequential Designed Mixed Research Method*

According to [9], the exploratory sequential design is a technique which carries out qualitative methods in data collection phase to explore broadly the relevant themes to a particular study. In our case, we carried out content analysis to gather relevant information for our research. The qualitative data were then analysed using quantitative instruments. The quantitative instrument that we used was the National Institute of Standards and Technology (NIST) Access Control System Evaluation Metrics. Based on our objectives, the following are the research questions to support our research:

RQ1: What are the issues with existing access control models for cloud computing?

RQ2: How good is the Zero-Trust Access Control Model compared to existing access control model based on NIST Metrics?

B. *Data Collection*

In our data collection phase, we used a qualitative data collection technique, content analysis, to gather relevant data from the literature that we used to compare different access control models. The content/document/studies selected and researched are based on the inclusion and exclusion criteria. The inclusion criteria include the research and studies on which the data extraction was performed. While exclusion criteria are the criteria which were used to exclude the content that are not related to our research. TABLE I shows the inclusion and exclusion criteria for our research.

TABLE I. INCLUSION AND EXCLUSION CRITERIA

Type	Criteria
Inclusion Criteria	• Studies that apply NIST criteria on access control models • Studies that discuss issues in access control model
Exclusion Criteria	• Studies in any other language than English • Duplicated studies • Studies that are not publicly available and have restriction to them

After the selection of studies to be used for our research we made a data extraction strategy to each study to gather relevant information from them. TABLE II shows the parameters used in our data extraction strategy.

TABLE II. DATA EXTRACTION PARAMETERS

Data Extracted	Description
ID	Unique id for each preferred study
Author	Name of the author of the study
Title	Title of the study
Year	Year of the publication
Type	Study type (Journal. Research Report, Conference Proceedings, Book Section)
Domain	Research domain (for example Artificial Intelligence, Software Engineering)
Methodology	The technique used to write the study e.g., case study, systematic review, empirical study, interview to get data, observation
Access Control Model	The access control method used discussed or used in the study of inspection
NIST Criteria	NIST criteria discussed in the study

C. *Analysis / Evaluation Metric*

The evaluation metric used in our research are the National Institute of Standards and Technology (NIST) Access Control System Evaluation Metrics [11]. NIST is a US (United State) based institute that establishes worldwide valid standards and scaling methods. The access control models in our research are evaluated based on these metrics. These tests provide a clearer view of the control characteristics to assess whether the model is sufficient. The following are the metrics that we used to evaluate and examine the controls or our models, these metrics are chosen as they are applicable to selected AC systems are shown in Table III-1.

Table III-1: NIST criteria relevant to selected Access Control Models.

ID	Name	Description
1	Privileges/Capabilities Discovery	It manages the representatives of the administration and addresses the issue of the supporting of activities conducted by individuals for these members.

2	Ease of privilege assignments	It is connected to the simplicity of the tasks that are carried out in the method.
3	Syntactic and semantic support for specifying AC rules	It addresses the problem whether somaticized or syntactic distinctions should be made while critical decisions are resolved.
4	Policy management	According to access rights, the values determined for each model must be developed.
5	Delegation of administrative capabilities	Access control will allow designated persons the ability to transfer their power to other individuals.
6	Flexibilities of configuration into existing systems	It investigates whether the device has significant output scalability/flexibility properties.
7	The horizontal scope of control	It verifies that the device has access between application, DBMS and OS.
8	The vertical scope of control	It verifies that the device is compliant with other platform frameworks.
9	Policy combination, composition, and constraint	It involves the access system's ability to integrate rules and content with certain restrictions in various policies.
10	Bypass	It looks at whether the legislation set for the management of entry to the system will resolve the crucial circumstances.
11	Separation of Duty (SoD)	It demands that entry to the machine be limited against a safety leak.
12	Safety	It determines if the access control has security measures to validate the leakage in the specified allowances.
13	Conflict resolution or prevention	It determines if there will be contradictions in the access authorization decisions that would be issued according to the demands.
14	Operational/situational awareness	It discusses the condition knowledge of the system, under which the system chooses to have access by deciding the concept that will apply.
15	Adaptable to the implementation and evolution of AC policies	Takes account of how well the structure can be tailored to evolving values and conditions in time.
16	Policy repository and retrieval	Offer details as to whether the system has suitable participants who help the system to work on the policy.

IV. Results and Justification

In this section of our report, we will answer two research question (RQ1 and RQ2) specified in the previous section.

The research question RQ1 seeks to justify the issues that exists in some of the most widely used access control models such as Role-Based Access Control (RBAC) model, Attribute-Based Access Control (ABAC) model and Mandatory Access Control (MAC) model. Table IV-1 highlights the issues that are currently faced by these three models. These issues are discussed in more details in the coming subsections.

Table IV-1: Issues in three most common access control models

Sr. No.	Model	Issues
1	Role-Based Access Control (RBAC)	• Role Explosion • RBAC Scalability • Security Risk Analysis Problem
2	Attribute-Based Access Control (ABAC)	• Policy Complexity • Auditability • Model Definition
3	Mandatory Access Control (MAC)	• Constant Maintenance • Lack of Access Convenience

A. RBAC Issues

RBAC model has several disadvantages in the real-world implementation.

1) Role Explosion

As a company or organization grows and gains more specialized departments, more roles are to be created under each department and more roles for each sub department. In some cases, a user may hold several roles and when they are replaced with other users, that user also gains all the roles that the previous user had. IT system administrators will either eventually be forgot to change their roles and just keep what it is now.

2) RBAC Scalability

As the situation above, more people entered the business, and the organizational charts and work definitions were not revised or clearly defined in the rush of onboarding all the new people. This most require the IT (Information Technology) system administrators to redesign the definitions to get the management role back on track.

3) Security Risk Analysis Problem

Risk analysis should be done once per period to make that system is always prevented from any malicious risks. Every time a permission is granted to a role to access a data in system, it possesses a risk. If the role or permission authorizer has no fundamentals or intimate knowledge on the security risk in system, it is extremely hard for IT administrators to maintain the security risks as the data is accessible from anyone who has the permissions, and these are not controlled by the IT administrators.

B. ABAC Issues

ABAC though seems better in efficiency than RBAC, it also comes with some drawbacks.

1) Policy Complexity

Policies can be very completed to determine especially in an environment with a lot of resources and information changing between subject and resources. IT system administrators must write and specify abundant of policies to determine the attributes that user can use to access the resources in the system [10].

2) Auditability

As users uses attributes and policy rules to access the resources, ABAC is also an identity-less access control system. In RBAC, the IT administrator can check the users who access the resources by simply checking the role and permissions but not for ABAC cases [11].

3) Model Definition

As what we discussed before, ABAC has not reach a unified opinion among the experts, and this has led to uncertainty of organization of which model of the experts' opinion that they should follow. Unstandardized model can lead to severe problems in the system if not implemented properly. This problem has also made ABAC less favourable and not much research can be done without abundant of data on it.

C. *MAC Issues*

The enforcement of security level in MAC has led to several disadvantages if compared to others.

1) Constant Maintenance

Due to the strong enforcement on security level, IT administrators must keep update and renew the security level time to time to make sure the access right is always restricted to certain users [12].

2) Lack of Access Convenience

Information exchange between various levels is not possible due to the access rights. Whenever a task is given, it can only be given to the users that are equal or higher in security level to access the resources [12].

D. *Comparison*

Now to answer the second research question, **RQ2**, we will be researching a relatively new Zero-Trust Access Control (ZTAC) model to overcome the issues with RBAC, ABAC and MAC models.

Zero Trust is a security principle and a structure focused on the premise that trust goes beyond the vicinity of the network and the endpoints connecting users to business systems. Trust is never presumed in a Zero Trust security model. It is instead proved by a variety of concerted acts, such as user identity and system checks. Table IV-2 depicts the evaluation of zero-trust access control model versus other three access control models based on evaluation criteria presented in Table III-1.

Table IV-2: Comparison among different access control models

ID	RBAC	ABAC	MAC	ZTAC
1	M	N/A	L	H
2	H	H	M	M
3	M	H	L	H
4	N/A	L	N/A	M
5	H	L	L	L
6	H	L	L	L
7	H	H	L	H
8	H	M	M	H
9	L	M	L	H
10	N/A	N/A	N/A	N/A
11	M	H	H	H
12	M	H	H	H
13	H	H	M	H
14	H	M	M	H
15	H	M	M	M
16	*	N/A	N/A	N/A

a. Legend (Low: L, Medium: M, High: H, *optional, Not Mentioned: N/A)

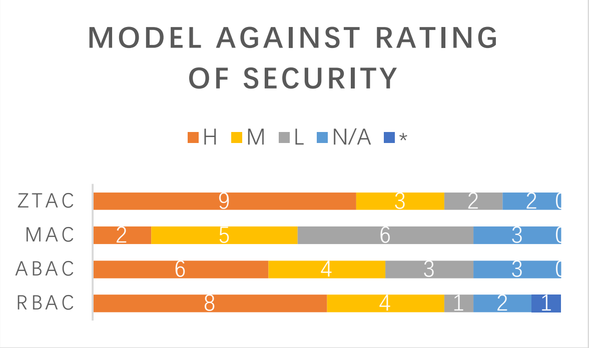

Figure IV.1: Chart of Model Against Rating of Security

Table IV-2 consist of four access control model that are rated with Low: L, Medium: M, High: H, *optional, Not Mentioned: N/A. Credit to G¨ozde Karatas and Akhan Akbulut [13], they have discussion on the RBAC, ABAC and MAC. We also went through other papers [14] that also discuss about RBAC, ABAC and MAC and get aspiration onto doing zero trust access control model for the comparison.

Zero trust access control model is based on articles in [15] [16] where the zero trust is be used in BeyondCorp which is introduced by Google. The basic idea of zero trust is not trusting anything in the network before access control engine and policy engine gives a trust to it. The zero-trust access control model uses inventory-based access control where the engine not only consider the user but also the devices and the network of the devices it is connected to. This gives the model high in *Privileges/Capabilities Discovery*, *horizontal and vertical scope of control,* and *Policy combination, composition, and constraint.* The model restricts users with many policies and level of permission to follow. Therefore, the model is a bit different to set for the policy and permissions where the *Policy Management and Ease of privilege assignments* is medium. *Flexibilities of configuration into existing systems* is low due to the extra permission and care required to focus on translating and adding device and network information.

According to [15], the *Delegation of administrative capabilities* is low due to the company assign the permission through company's HR department only. Others are not allowed to change their permission except where is allowed.

Separation of Duty (SoD) is high because the will model reset the trust and access of user of a particular device on a particular network after being disconnected for a long time. *Conflict resolution or prevention, Operational/situational awareness* and *Adaptable to the implementation and evolution of AC policies* are high because the framework has set "Migration Strategy" to mitigate with almost all condition it will meet. The *Bypass* and *Policy repository and retrieval* are not stated in the papers.

V. CONCLUSION

The best of all is the zero-trust access control model which give high confidence in scoring almost all the expectations given to it while others are lack behind. There are other access models that evolve from RBAC, MAC and ABAC that are not discuss in this paper. All in all, the result we have matches our expectation where the zero-trust access control model score the best but have a short in some places.

Limitation of this method is the limitation of number of research papers and the correctness of the papers. There are also unknown attributes that can be tested. For future research, the further comparison among the models is required where more models are taking into the consideration.

REFERENCES

[1] R. S. Sandhu and P. Samarati, "Access Control: Principles and Practice," *IEEE Commun. Mag.,* vol. 32, pp. 40-48, 1998.

[2] P. K, “Analysis of Different Access Control Mechanism in Cloud,” *International Journal of Applied Information Systems,* vol. IV, no. 2, pp. 34-39, 2012.

[3] D. F. Ferraiolo and R. D. Kuhn, “Role-Based Access Controls,” National Institute of Standards and Technology, Gaithersburg, 1992.

[4] R. Sandhu, D. Ferraiolo and R. Kuhn, “The NIST Model for Role-Based Access Control,” National Institute of Standards and Technology, 2000.

[5] D. F. Ferraiolo, D. R. Kuhn and R. Chandramouli, Role-Based Access Control Second Edition, Norwood: ARTECH HOUSE, INC, 2007.

[6] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller and K. Scarfone, “Guide to Attribute Based Access,” National Institute of Standards and Technology, Gaithersburg, 2014.

[7] K. DelBene, M. Medin and R. Murray, “The Road to Zero Trust (Security),” *Defense Innovation Board,* pp. 1-10, 1 October 2019.

[8] Microsoft, “Zero Trust Maturity Model,” *Microsoft Security,* 2019.

[9] M. M. Lesly A. Dossett, M. P. Amy H. Kaji and M. M. Justin B. Dimick, “Practical Guide to Mixed Methods,” *JAMA Surg.,* pp. 254-255, 2020.

[10] T. Keary, “Comparitech,” Comparitech Limited, 1 July 2020. [Online]. Available: https://www.comparitech.com/net-admin/rbac-vs-abac/. [Accessed 7 December 2020].

[11] D. Servos and S. L. Osborn, “Current Research and Open Problems in Attribute-Based Access Control,” *ACM Computing Surveys,* p. January, 2017.

[12] “Mandatory Access Control vs Discretionary Access Control: Which to Choose?,” 11 March 2020. [Online]. Available: https://www.ekransystem.com/en/blog/mac-vs-dac. [Accessed 10 December 2020].

[13] G. Karatas and A. Akbulut, “Survey on Access Control Mechanisms,” *Journal of Cyber Security and Mobility,* vol. 7, no. 3, p. 1–36, 2018.

[14] Y. A. Younis, K. Kifayat and M. Merabti, “An access control model for cloud computing,” *Journal of Information Security and Applications,* pp. 1-16, 2014.

[15] R. Ward and B. Beyer, “Beyondcorp : a new approach to enterprise security,” *;login:: the magazine of USENIX & SAGE,* vol. 39, no. 6, pp. 6-11, 2014.

[16] M. Campbell, “Trust Is a Vulnerability,” *Ieee,* 2020.

[17] V. C. Hu and K. Scarfone, “Guidelines for Access Control System Evaluation Metrics,” *National Institute of Standards and Technology,* pp. 1-32, 2012.