International Journal on Advanced Science Engineering Information Technology

Vol.14 (2024) No. 1
ISSN: 2088-5334

ABAC as Access Control Solution for Digital Evidence Storage

Tri Kuntoro Priyambodo [a,*], Yudi Prayudi [b], Rahmat Budiarto [c]

[a] *Department of Computer Science and Electronics, Gadjah Mada University, Yogyakarta, 55281, Indonesia*
[b] *Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia*
[c] *College of Computer Science and IT, Albaha University, Saudi Arabia*
*Corresponding author: *mastri@ugm.ac.id*

***Abstract*— Digital evidence is content that must be protected against access and use by parties who should not have the authority to do so. Some protection parameters for access to digital evidence must be implemented to ensure its integrity and authenticity. Access to digital evidence is not enough to be facilitated only with authorization and authentication mechanisms but must also be facilitated with other aspects of access by users according to their level of authority. One approach is to use the concept of access control. The study of access control to digital evidence is essential. However, studies on this matter are still limited. Among the many access control models, the application of access control based on attribute variations is a concept that can be applied to the context of access to digital evidence. This paper discusses policy design and modeling using attribute-based access control (ABAC) with four attributes: subject, resource, action, and environment. Then, it implements and tests various requests to the system based on attribute variations and possible algorithms. This study supports the security of digital evidence storage systems through access control to the resources it manages using the Policy Statement, Policy Modeling, Policy Implementation, and Policy Validation approaches. The application of the access control design shows that the ABAC concept has been successfully applied as an access control solution for digital evidence stored in digital evidence storage systems. The built policy design was successfully validated using ACPT Tools, concluding that there was no inconsistency or incompleteness.**

***Keywords*— Forensics; digital evidence; access control; storage; ABAC.**

Manuscript received 27 Mar. 2022; revised 14 Aug. 2023; accepted 3 Jan. 2024. Date of publication 29 Feb. 2024.
IJASEIT is licensed under a Creative Commons Attribution-Share Alike 4.0 International License.

I. INTRODUCTION

As a result of the development of electronic devices and information technology, the digital age has raised another problem in the form of cybercrime. Cybercrime is a criminal activity carried out by utilizing electronic devices and the availability of information technology as an instrument to support its activities [1]. The number of cases and losses caused by cybercrime activity has increased from year to year [2]–[4].

A series of digital forensics stages support efforts to disclose cybercrime cases through digital investigative activities to obtain evidence relevant to the investigation case. Digital forensics itself, according to [5] and [6], is an activity based on scientific methods and the application of forensic principles to digital evidence so that it becomes a support for legal evidence and trials. The critical factor in a cybercrime investigation process is related to evidence divided into electronic and digital evidence [7], [8]. Based on the literature review, there are three main problems relating to evidence: storing evidence, recording contextual information on the evidence, and controlling the accessibility [9], [10].

Digital evidence is a digital source that must be closely guarded for access and use through an appropriate access control mechanism. The centralization mechanism for digital evidence storage is an essential issue in supporting digital evidence control in line with the opinion of [11] and [12] about the importance of evidence storage mechanisms as part of evidence control mechanisms. Centralization will make it easier to implement access control schemes for resources.

One of the studies on evidence storage is done by [13]. However, this research only discusses solutions for secure storage models for digital evidence. The paper does not discuss the issue of how to secure access to evidence storage. This paper has not further studied the issue of access control for digital evidence storage. Likewise, other papers that discuss current issues of digital forensics, such as in [14] and [15], missed the point of access control for digital evidence storage. This fact shows that studying access control for

digital evidence storage as part of digital forensics is still not a concern for researchers.

Regarding access control, accessibility can be implemented in the physical environment through a permitting mechanism to enter and leave the room and certain authorities attached to each officer. Within the scope of digital evidence handling, this issue can be approached by applying the access control policy concept to the digital evidence stored. Based on the literature review, the issue of access control for digital evidence is an open problem in digital forensics [16], [17]. The access control of digital evidence is insufficient to be handled only by the authentication and user authorization mechanisms. Authentication, authorization, and access control have different functions and objectives, even though the implementation looks like a single process.

According to [18], authentication focuses on verifying user identity claims. Authorization focuses on granting access rights to resources. In contrast, access control focuses on protecting the security of specific resources, a mechanism to ensure that users do not act on certain things that do not follow the general security policy. Access control protects the system and resources from unauthorized access and determines the authorization level after completing the authentication procedure.

Previous research on the chain of custody for digital evidence has developed a solution for digital evidence storage through a system identified as the Digital Evidence Storage Imaginary Cabinets system [7], [19]. The existing access control in digital evidence storage is only an authentication and authorization process for the username and password. In contrast, the access control model offers a more complex authentication and authorization process by applying policies as access settings. Digital evidence storage contains the technical dimensions of storage space and digital evidence management and regulates access to systems and resources. Building an access control policy concept suitable for digital evidence accessibility is a research challenge that will be explored in this paper.

Considering there is no scheme for access control models in digital evidence storage, it is necessary to design a policy and model of access control using the attribute-based access control approach. The solution discussed in this paper to overcome the problem of access control in digital evidence storage cabinets is through the attribute-based access control (ABAC) model as a new generation of access control concepts. This concept has the flexibility of the design of access control. It is also the development of existing access controls such as discretionary access control (DAC), mandatory access control (MAC), access control list (ACL), and role-based access control (RBAC).

Here, we need to adopt a more flexible access control approach that allows defining attributes for entities and environmental conditions (e.g., time, location, etc.) and specify access control policies based on those attributes [20]. For this reason, building an access control policy suitable for digital evidence accessibility is a study that needs further exploration. This research creates an attribute-based access control model as an access control policy to provide access rights for users with the authority to handle digital evidence in digital evidence storage.

In particular, the context of this research is on managing digital evidence within the scope of law enforcement in Indonesia. The existing regulations are still oriented towards physical evidence and require a control mechanism for the accessibility of physical evidence. Meanwhile, digital evidence has different characteristics from physical evidence. For this reason, the research results discussed in this paper can be a solution to support the application of existing regulations in the digital evidence environment.

In particular, the context of this research is on managing digital evidence within the scope of law enforcement in Indonesia. The existing regulations are still oriented towards physical evidence and require a control mechanism for the accessibility of physical evidence. Meanwhile, digital evidence has different characteristics from physical evidence. For this reason, the research results discussed in this paper can be a solution to support the application of existing regulations in the digital evidence environment.

II. Material and Method

Access control is a mechanism to limit the operation or action of a computer system to only legitimate users [21]. Meanwhile, access control has four main issues: identification, authentication, authorization, and access decisions. A brief explanation is as follows:

- Identification: identify the party responsible for the access request. It can be a person or NPE (non-person entity), such as a computer or application.
- Authentication is confirming the truth of a piece of data or an entity. User Authentication itself means confirming user data that has previously been stored.
- Authorization: this process determines what services are allowed to be used by users whose identity is clear (authenticated user).
- Access Decision: based on a combination of the three aspects above, a decision is made on whether the request is permitted or the system processes it.

The concept of access control primarily determines the integrity and credibility of digital evidence applied to it. Therefore, the mechanism for digital evidence protection that supports the integrity, confidentiality, and authenticity of digital evidence is essential. In this case, within a policy scope, access control indicates whether a subject (i.e., process, computer, user, device) allows or not to operate (e.g., read, write, execute, delete, search) of an object (e.g., database, table, file, service, resource). Meanwhile [illegible], access control is a mechanism that only authorizes legitimate users to take advantage of existing data and resources.

The application of access control to digital evidence has been suggested previously by Hsu and Lin [16] through a model applying cryptographic techniques to the hierarchical access control mechanism. In this case, a partial and complete supervision mechanism is developed to describe the different rights and functions of the investigator who directly handles digital evidence and other law enforcers who exercise control over the use of the evidence. The solutions provided in that study focus on controlling and protecting access to digital evidence by applying AES cryptography at different security levels.

Furthermore, access control for a chain of custody is similar to the access control issue for medical records in a Healthcare Information System. In this case, [24], [25] it provides a solution for the access control model for a collaborative environment in medical records. The analogy applied is a condition where several doctors from different departments handling a patient can access a medical record. This solution allows a record stored in a single database to be shared with other parties as long as it matches its role in the organization. The healthcare system is an excellent example of a distributed collaborative environment where interventions such as doctors, administrators, and nurses collaborate to provide care to patients more efficiently. However, these systems pose new challenges regarding who can access, collaborate, and share data and under what conditions. Confidentiality, unauthorized access to medical data, and collaborative processes are among the main concerns that require adequate attention during all stages of system development. Role-Based Access Control (RBAC) is modified to support collaborative work with team and task models. Medical Activity Dominance is defined as role dominance in the RBAC model.

Security issues regarding digital evidence are generally approached by the concept of a secure environment, both in obtaining digital evidence or maintaining the integrity of the digital evidence itself [13]. However, one of the critical issues in the security of digital evidence is the issue of access control of digital evidence stored in particular storage media. Another proposed solution [13] is the concept of Block Proof as a framework for verifying the authenticity and integrity of web content.

Based on the literature review, the discussion around access control of digital evidence is an open problem in digital forensics. Some of the discussions include the requirements needed when interacting with digital evidence, as presented by [26] and [27], and the use of the Attribute-Based Access Control (ABAC) model to explain access control policies and XACML as an implementation of the policy language used as a hierarchical access control model proposed by [16]. Furthermore, despite the different domains, several access control solutions in the medical record/health record submitted by [25], [28] can be used to build access control solutions relevant to digital evidence.

The Extensible Access Control Modelling Language (XACML) modeling language was developed to implement the ABAC access control policy. XACML is an XML-based access control policy language notable for supporting attribute-based policies and used in multiple access control products. XACML is a policy language capable of constructing expressions from a series of policy access controls so that it can explain: “who can do, what and when”.

Fig. 1 shows the stages of applying the access control concept to digital evidence storage. This research uses UMU Editor and ACPT as policy modeling tools. UMU Editor is applied to develop Policy Modeling, while ACPT is applied for Policy Validation. ACPT is a tool developed by NIST as a proof of concept of policy testing issued by NIST

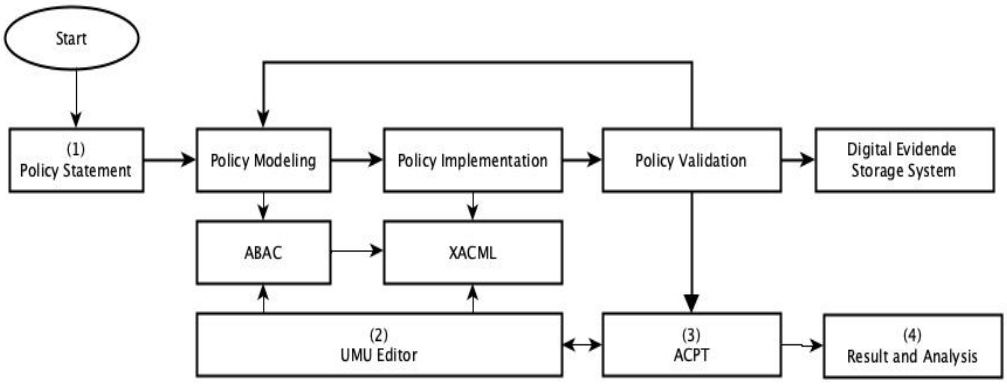

Fig. 1 The state of development of the Access Control Model

Based on the illustration in Fig. 1, the first step (1) is to identify the policy statement applied to the digital evidence storage system. Furthermore, (2) uses the ABAC approach and UMU Editor tools to conduct policy modeling based on agreed attributes. This modeling results from an XACML output used as part of an access system for digital evidence storage systems. After successfully implementing, the next step (3) is to validate the policy statement using the ACPT tools. The final step (4) is to analyze the results of the policy statement development that has been made and the validation results.

A. Policy Statement

The first step to building an Access Control Policy is to prepare a policy statement suitable for the Digital Evidence Storage system. Policy statements are designed based on the central concept of ABAC: they do not permit the output of a direct relationship between subject and object, but permission is granted through both attributes [20].

The scenario was designed using a digital evidence storage system with the following:

- The main actors as subjects consist of the first responder, examiner, officer, and external.
- There are two environmental attributes: Registered and Non-Registered.
- Six action attributes: Upload, Create, Input, Download, Delete, Validate.
- Nine resource attributes: Digital Evidence, Cabinet, Rack, Bag, Data Evidence, Data Case, Username/Password, Form CoC, and Signature.

Furthermore, the policy statement that will be applied to the digital evidence storage system is as follows:

1) First Responder. This actor can log in to the system when it fulfils the policy component. The subject contains the work status identity relevant to the environment that the system has determined in the form of IP address registration, time access, and Mac address. Furthermore, if the subject and environment are appropriate, the resources provided are cabinet, rack, bag, digital evidence, and data evidence, with actions such as create, upload, and input. After being declared to fulfil all policies, this actor can access the system following its function and role.

2) Examiner. This actor can log in to the storage system when it meets the policy component. The subject contains the job status identity relevant to the environment specified by the system in the form of IP address registration, time access, and Mac address. Furthermore, if the subject and environment are appropriate, the resource given is data case and digital evidence with actions in input and download. After being declared to fulfil all policies, this actor can access the storage system following their functions and roles.

3) Officer. This actor can log in to the storage system when it meets the policy component. The subject contains the job status identity relevant to the environment specified by the system in the form of IP address registration, time access, and Mac address. Furthermore, suppose the subject and environment are appropriate. In that case, the given resources are username, signature, cabinet, digital evidence, data evidence, data case, and CoC form with actions such as create, delete, validate, and download. After being declared to fulfill all policies, this actor can access the storage system following their functions and roles.

4) External. This actor can log in to the storage system when it meets the policy component. The subject contains the job status identity relevant to the environment specified by the system in the form of IP address registration, time access, and Mac address. Furthermore, if the subject and environment are appropriate, the resource provided is digital evidence and the Chain of Custody form, with action in the form of downloads. After being declared able to fulfill all policies, this actor can access the storage system following their functions and role.

B. Attribute-Based Access Control (ABAC)

The next step is to translate the policy statement into a rule. Policy and rules have a significant role in designing attribute-based access control. Policy and rules will map every attribute in the access control element. In this case, the attribute will function as a policy rule when the request is made. Tables 1-4 list the design rules for the attributes used in the digital evidence storage imaginary cabinets system. Based on Table 1, Table 2, Table 3, and Table 4, 18 rules for attribute mapping will function as policy rules when the request is made.

TABLE I
THE RULES FOR THE FIRST RESPONDER FOR ACCESS TO THE DIGITAL EVIDENCE STORAGE SYSTEM

Resource	Actions	Environment	Decision
Cabinet	Create	Registered Environment	Permit
		Non-Registered Environment	Deny
Rack	Create	Registered Environment	Permit
		Non-Registered Environment	Deny
Bag	Create	Registered Environment	Permit
		Non-Registered Environment	Deny
Digital Evidence	Upload	Registered Environment	Permit
		Non-Registered Environment	Deny
Data Evidence	Input	Registered Environment	Permit
		Non-Registered Environment	Deny

TABLE II
THE RULES FOR EXAMINERS FOR ACCESS TO A DIGITAL EVIDENCE STORAGE SYSTEM

Resource	Actions	Environment	Decision
Username	Create	Registered Environment	Permit
		Non-Registered Environment	Deny
Password	Create	Registered Environment	Permit
	Create	Non-Registered Environment	Deny
Signature	Create	Registered Environment	Permit
		Non-Registered Environment	Deny
Digital Evidence	Delete	Registered Environment	Permit
		Non-Registered Environment	Deny
Digital Evidence	Validate	Registered Environment	Permit
		Non-Registered Environment	Deny
Data Evidence	Validate	Registered Environment	Permit
		Non-Registered Environment	Deny
Data Case	Validate	Registered Environment	Permit
		Non-Registered Environment	Deny
Form CoC	Create	Registered Environment	Permit
		Non-Registered Environment	Deny
Form CoC	Download	Registered Environment	Permit
		Non-Registered Environment	Deny

TABLE III
THE RULES FOR OFFICERS FOR ACCESS TO A DIGITAL EVIDENCE STORAGE SYSTEM

Resource	Actions	Environment	Decision
Data Case	Input	Registered Environment	Permit
		Non-Registered Environment	Deny
Digital Evidence	Download	Registered Environment	Permit
	Download	Non-Registered Environment	Deny

TABLE IV
THE RULES FOR EXTERNAL ACCESS TO A DIGITAL EVIDENCE STORAGE SYSTEM

Resource	Actions	Environment	Decision
Form CoC	Download	Registered Environment	Permit
		Non-Registered Environment	Deny
Digital Evidence	Download	Registered Environment	Permit
		Non-Registered Environment	Deny

An ABAC policy represents a function that determines whether an access request is allowed based on the given attribute value. Formally an ABAC policy will contain a triple (X, Y, F). Where:

- X is the finite set of attributes with domain D1 ... Dn
- Y is the finite set of access control decisions (for example, permit, deny, undefined)
- F: = D1 x D2 x ... Dn ⇒ Y; access control function

Based on the information in Table I, then:

D1 = The set of attributes for the subject = {First Responder, Examiner, Officer, External}

D2 = The set of attributes for the environment = {Registered, non-registered}

D3 = The set of attributes for the actions = {Upload, Create, Input, Download, Delete, Validate}

D4 = The set of attributes for the resource = {Digital Evidence, Cabinet, Rack, Bag, Data Evidence, Data Case, Username/Password, Form CoC, Signature}

So, the formal notation for the ABAC rule in the Digital Evidence Storage Imaginary Cabinets System is:

F = (The set of Subject Attribute) x (The set of environment Attribute) x (The set of Action Attribute) x (The set of Resource Attribute) ⇒ Y (Permit, Deny)

The meaning of that notation is subject; if it meets the required environment, the subject will be permitted to perform specific actions on a particular resource. If the environmental conditions are not met, or the act on a resource is unjustified, the status is Deny.

The ABAC design details the policy statement as the basis for access control for each Digital Evidence Storage System user. In this case, the ABAC in the Digital Evidence Storage System is analogous to a login process in which the authentication process is through the policy rules embedded in the actor as the subject and the application as an object. The concept of access control must be able to identify each characteristic of users who access the application. The identification is based on the policy rules made and stored as XACML structures.

C. Policy Implementation

After the ABAC design in the system of Digital Evidence Storage is made, the next step is to prepare the implementation scheme through the access control implementation prototype model. Fig. 2 shows an overview of the previously designed access control implementation.

The next important step is to apply the access control policy architecture to the XACML structure with the system architecture in Fig. 3. In Fig. 3; it is explained that the XACML model will contain two main entities, namely Policy Enforcement Point (PEP) and Policy Decision Point (PDP). PEP is the primary entity that will protect the resource. PEP will accept access requests and forward them to PDP. Furthermore, PDP will make decisions according to the information contained in the request in the XACML context. Each request defines the subject, environment, action, and resource, which are summarized into a set of attributes.

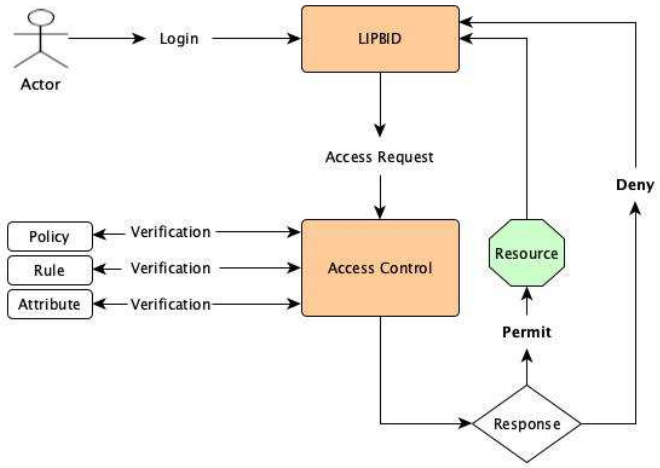

Fig. 2 The Overview of Access Control Implementation

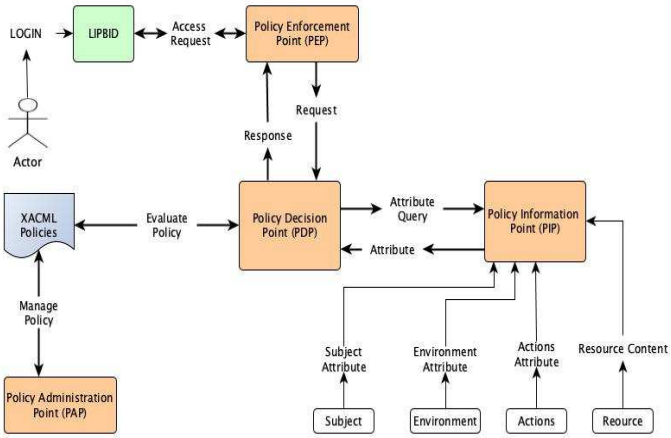

Fig. 3 XACML Policy Data Flow Model

The XACML of Digital Evidence Storage Imaginary Cabinets System, a data flow model, is a logical description of processing an access request. Policy Enforcement Point (PEP), when an access request is made, the initial executor, will provide a request to the Policy Decision Point (PDP) to decide on the request for action. Furthermore, the Policy Information Point (PIP) contains four attributes: subject, resource, actions, and environment. In this case, the Policy Decision Point (PDP) has a function to evaluate XACML policies in the Policy Administration Point (PAP) and functions to manage XACML policies.

The implementation of XACML in the Digital Evidence Storage system includes XACML output in two parts of the program in the subject and environment for the authorization and user validation processes and the central part of program services for access to resources and actions. Only users who meet all the rules can access the system and use the resources and actions that match its rules. The result is a Digital Evidence Storage system report for user login failures due to inappropriate subjects and environment. In contrast, a successful login activity will be part of the access record in the generated chain of custody form.

III. Result and Discussion

ABAC is flexible and can accommodate various attributes relevant to policy statements designed for specific needs. However, the complexity of the applied policies allows the emergence of conditions of inconsistency and incompleteness. This condition occurs when the user should have permissions in the form of a permit, but the evaluation output produces a value in the form of denial, and vice versa. From the aspect of computer security, in the opinion of [21], [30], attacks against the system occur because of inconsistencies in the implementation of access control.

The tool used for policy validation in this study is the NIST-developed ACPT. The policy statements and rules as contained in Table 1-4, then translated into the ACPT system. Among the validation algorithm combinations provided by ACPT are the following:

- First applicable, the condition where the policy statement has been compiled and provides the final permit value will be prioritized to be executed.
- Deny overrides, which is a condition if there is a combination of a policy statement such that if there is a decision between a permit and deny, then a decision is preferred.
- Permit override is the opposite of deny overrides, a combination of policy statements such that if there is a final decision on the permit, then the final value of the permit takes precedence.

A simple policy validation test uses a combination of the first applicable algorithm, deny override and permit override, each carried out 30 times testing according to the minimum number of samples for large populations. This test ensures the prepared policy statement is protected from inconsistency and incompleteness. In each algorithm test, ACPT tools will produce 60 different attribute value combinations in this case. The value of 60 is a standard setup of the 2011 version of ACPT used in this study. Table 5 is a summary of the outputs from the ACPT test results.

Based on the result data, then by referring to the definition of inconsistency and incompleteness, the following facts are obtained:

- No output is found with the condition that there are two or more combinations of rules (subject, environment, action, resource) $\Rightarrow$ (Permit, Deny), which gives a different final value. Thus, inconsistency is a condition where two rules give contradictory results, and it turns out that it is not fulfilled.
- There are no outputs with combinations that have not been defined before. Thus, the condition of incompleteness, namely the existence of conditions where there are rules that have not been accommodated in a set of rules that have been previously defined, is not fulfilled.

Under these conditions, the policy statement to be applied to the Digital Evidence Storage system matches the expected access control policy. Testing about inconsistency and incompleteness for the ABAC access control policy conducted in this study is still straightforward. Testing is only based on a simple combination of existing algorithms using ACPT tools (released in 2011). The overall results of the simulation output mapping show that not all attribute combinations appear.

TABLE V
SUMMARY OF ACPT RESULT OUTPUT

No of Trial	First Applicable		Deny Override		Permit Override	
	Permits	Deny	Permits	Deny	Permit	Deny
1	3	57	2	58	3	57
2	2	58	3	57	2	58
3	2	58	2	58	1	59
4	4	56	1	59	2	58
5	2	58	2	58	2	58
6	2	58	2	58	3	57
7	2	58	2	58	3	57
8	3	57	4	56	3	57
9	3	57	2	58	3	57
10	2	58	3	57	2	58
11	1	59	1	59	1	59
12	1	59	3	57	1	59
13	2	58	2	58	4	56
14	4	56	2	58	3	57
15	2	58	1	59	2	58
16	2	58	4	56	1	59
17	3	57	3	57	2	58
18	3	57	2	58	1	59
19	3	57	2	58	2	58
20	3	57	3	57	2	58
21	1	59	2	58	4	56
22	1	59	2	58	1	59
23	3	57	1	59	2	58
24	2	58	3	57	1	59
25	2	58	1	59	3	57
26	1	59	1	59	1	59
27	4	56	2	58	1	59
28	2	58	2	58	5	55
29	2	58	2	58	1	59
30	2	58	3	57	2	58

Thus, the conclusion about inconsistency and incompleteness of the policy statement is based on the output produced by the ACPT in this study. Originally, ACPT was a tool for the proof of concept of policy testing and is a research-based tool. ACPT then changed to Commercial Security Policy Tools (SPC) with more complex algorithmic combination capabilities in its development.

One of the preliminary studies on applying access control in the scope of digital evidence refers to his research [16] through a model of applying cryptographic techniques to the hierarchical access control mechanism. In this case, [16] a partial and complete supervision mechanism was developed to describe the different rights and functions of investigators who directly handle digital evidence and other law enforcers who exercise supervisory control over the use of such evidence. The solution is more focused on efforts to control and protect access to digital evidence by applying AES cryptography at different security levels.

In principle, the concept of access control from [16] gives public-private keys and signatures to each user that is different according to their authority so that only those with the authority can access digital evidence. This solution is an extension of user authorization techniques. Digital evidence is protected by applying cryptographic techniques to the digital evidence itself. Then, each user with the authority will have their public /private key and signature to open and access the digital evidence. Thus, the solution [16] is more of an extension of user authorization techniques through the provision of public/private keys and signatures that differ according to the level of the user. This aligns with the opinion that access control is a mechanism that only authorizes legitimate users to take advantage of existing data and resources.

This is different from the concept of access control in a digital evidence storage system through the ABAC approach. ABAC views access not only in obtaining digital evidence but also in actions against digital evidence. By applying a combination of rules (subject, environment, action, resource) $\Rightarrow$ (Permit, Deny), the concept of access control is more flexible but still controlled. The main strength of ABAC is in the design of policies that provide different actions for each protected resource. This is not found in the solutions provided by [16].

The concept of access control developed in this study is in line with the opinion of [32], which states that access control shows whether a subject (i.e., process, computer, user, device) allows or not to operate (i.e., read, write, execute, delete, search) on an object (i.e., database, table, file, service, resource). The difference between the concept of access control applied to the digital proof environment as proposed [16] and the ABAC access control concept applied to the Digital Evidence Storage Imaginary Cabinets system is presented in Table 6.

The access control approach in this research illustrates that access to important content and digital evidence must consider many aspects. This concept generally applies to access to all critical objects stored in a storage medium. The solution provided through the combination of attributes in ABAC using subject, resource, action, and environment produces certain decisions that are the basis for granting authorization access to digital evidence storage systems.

According to [23], it has several better features than models in the previous generation as a new generation of access control models. Based on the prototype ABAC implementation on a digital evidence storage system, we obtain several more comprehensive explanations about ABAC, that are:

- ABAC allows access control to be granted by combining several attributes from authorization elements such as subject, resource, action, and environment into one access control decision. This technique also allows the broadest possible scope of subjects to access the broadest possible range of resources without any individual relationship between each subject and each resource.
- ABAC facilitates collaborative policy administration within a large organization or between different organizations. Policymakers can compile individual policies from various departments or different organizations. In a large corporation, different departments can manage policy authorization elements.
- ABAC facilitates decoupling access control of the business logic of a particular application. This will cause an increase in the dynamic nature of access control. If the access control decision is separate from the application code, changes to the access control policy will cause minimal modifications to the application code.

Furthermore, ABAC is compatible with previous traditional access control concepts such as DAC, MAC, ACL and RBAC.

TABLE VI
COMPARISON OF ACCESS CONTROL CONCEPT

No	Component	Hsu and Lin	ABAC
1	Object	Encrypted Digital Evidence	Digital evidence stored in Digital Evidence Storage
2	Subject	The subject has a private/public key and signature to access digital evidence.	The subject requests an Object.
3	Decision	If the keys match, then the subject can access digital evidence.	The decision is made through an evaluation mechanism for (a) rules, (b) subject attributes, (c) object attributes, and (d) environmental conditions.
4	Output	Can be opened or not the encryption key from digital evidence	Deny or permit access to the object

IV. CONCLUSION

ABAC is an access control method where subjects can only make requests to carry out operations on objects based on the attributes embedded in the subject, object, environmental conditions, and the collection of policies included in the attributes and conditions. The authorization element is defined in the terminology attribute in the ABAC system. The attribute is a characteristic previously defined by the entity authorized to define policy.

In this study, the ABAC concept has been successfully applied as an access control solution for digital evidence stored in digital evidence storage systems. The built policy design was successfully validated using ACPT Tools, concluding that there was no inconsistency or incompleteness. It can be concluded that the design for the case on the system used as a prototype follows the needs of the access control policy. The design of the access control policy can be developed by expanding the scope of the flow model of digital evidence access. The more parties involved in accessing digital evidence, the more complex the access control policy will be, and the more a broader validation mechanism will be required.

ACKNOWLEDGMENT

This research is funded by the Ministry of Research and Technology/National Research and Innovation Agency for Universitas Gadjah Mada with contract number 2085/UN1/DITLIT/DIT-LIT/PT/2020.

REFERENCES

[1] C. Cross, T. Holt, A. Powell, and M. Wilson, "Trends & Issues in Crime and Criminal Justice," *Aust. Inst. Criminal.*, no. 635, 2021.

[2] (World Economic Forum), "Global Cybersecurity Outlook 2022," Geneva Switzerland, 2022.

[3] ICCC FBI, "Internet Crime Report 2021," USA, 2022.

[4] IBM Security, "X-Force Threat Intelligence Index 2022," 2022.

[5] G. Horsman, "Standardising digital forensic examination procedures: A look at Windows 10 in cases involving images depicting child sexual abuse," *WIREs Forensic Sci.*, vol. 3, no. 6, pp. 1–12, 2021, doi:10.1002/wfs2.1417.

[6] V. Roussev, "Forensics Knowledge Area Version 1.0.1," New Orleans USA, 2021.

[7] Y. Prayudi, A. Ashari, and T. K. Priyambodo, "The Framework to Support The Digital Evidence Handling : A Case Study of Procedures for The Management of Evidence in Indonesia," *J. Cases Inf. Technol.*, vol. 22, no. 3, pp. 51–71, 2020.

[8] Y. Prayudi, A. Ashari, and T. K. Priyambodo, "The Pseudo Metadata Concept For The Chain of Custody of Digital Evidence," *Int. J. Electron. Secure. Digit. Forensics*, vol. 11, no. 4, pp. 395–419, 2019.

[9] G. Horsman, "Digital evidence and the crime scene," *Sci. Justice*, vol. 61, no. 6, pp. 761–770, 2021, doi: 10.1016/j.scijus.2021.10.003.

[10] P. Reedy, "Interpol review of digital evidence 2016 - 2019," *Forensic Sci. Int. Synerg.*, vol. 2, pp. 489–520, 2020, DOI: 10.1016/j.fsisyn.2020.01.015.

[11] D. Kim, S.-Y. Ihm, and Y. Son, "Two-Level Blockchain System for Digital Crime Evidence Management," *Sensors 2021*, vol. 21, no. 3051, pp. 1–17, 2021, doi: 10.4324/9780429292767-22.

[12] European Union Agency for Law Enforcement Cooperation, "Evidence Situation Report 3rd Annual Report," 2021.

[13] A. Singh, R. A. Ikuesan, and H. Venter, "Secure Storage Model for Digital Forensic Readiness," *IEEE Access*, vol. 10, pp. 19469–19480, 2022, doi: 10.1109/access.2022.3151403.

[14] A. Al-Dhaqm *et al.*, "Digital Forensics Subdomains: The State of the Art and Future Directions," *IEEE Access*, vol. 9, pp. 152476–152502, 2021, doi: 10.1109/access.2021.3124262.

[15] F. Casino *et al.*, "Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews," *IEEE Access*, vol. 10, pp. 25464–25493, 2022, doi: 10.1109/access.2022.3154059.

[16] C. Hsu and Y. Lin, "A Digital Evidence Protection Method with Hierarchical Access Control Mechanisms," in *IEEE International Carnahan Conference on Security Technology (ICCST)*, 2011, pp. 1–9.

[17] N. Juma, X. Huang, and M. Tripunitara, "Forensic Analysis in Access Control: Foundations and a Case-Study from Practice," *Proc. ACM Conf. Comput. Commun. Secure.*, pp. 1533–1550, 2020, DOI: 10.1145/3372297.3417860.

[18] K. Erikson, "Frameworks for Centralized Authentication and Authorization," Åbo Akademi University, 2020.

[19] Y. Prayudi, A. Ashari, and T. K. Priyambodo, "The pseudo metadata concept for the chain of custody of digital evidence," *Int. J. Electron. Secure. Digit. Forensics*, vol. 11, no. 4, 2019, doi:10.1504/ijesdf.2019.102554.

[20] S. Bhatt, T. K. Pham, M. Gupta, J. Benson, J. Park, and R. Sandhu, "Attribute-Based Access Control for AWS Internet of Things and Secure Industries of the Future," *IEEE Access*, vol. 9, pp. 107200–107223, 2021, doi: 10.1109/access.2021.3101218.

[21] S. Kern, T. Baumer, S. Groll, L. Fuchs, and G. Pernul, "Optimisation of Access Control Policies," *J. Inf. Secur. Appl.*, vol. 70, no. September, 2022, doi: 10.1016/j.jisa.2022.103301.

[22] A. Singh, R. A. Ikuesan, and H. Venter, "Secure Storage Model for Digital Forensic Readiness," *IEEE Access*, vol. 10, pp. 19469–19480, 2022, DOI: 10.1109/access.2022.3151403.

[23] B. Kim, W. Shin, D. Y. Hwang, and K. H. Kim, "Attribute-Based Access Control (ABAC) with Decentralised Identifier in the Blockchain-Based Energy Transaction Platform," *Int. Conf. Inf. Netw.*, vol. 2021-Janua, pp. 845–848, 2021, doi:10.1109/ICOIN50884.2021.9333894.

[24] R. Barhoun, M. Ed-Daibouni, and A. Namir, "An extended attribute-based access control (ABAC) model for distributed collaborative healthcare system," *Int. J. Serv. Sci. Manag. Eng. Technol.*, vol. 10, no. 4, pp. 81–94, 2019, doi: 10.4018/ijssmet.2019100105.

[25] S. Khan *et al.*, "An Efficient and Secure Revocation-Enabled Attribute-Based Access Control for eHealth in Smart Society," *Sensors*, vol. 22, no. 1, pp. 1–23, 2022, doi: 10.3390/s22010336.

[26] Y. Dahiya and S. Sangwan, "Developing and Enhancing the Security of Digital Evidence Bag," *Int. J. Res. Stud. Comput. Sci. Eng.*, vol. 1, no. 2, pp. 14–25, 2014.

[27] J. Rajamäki and J. Knuuttila, "Law Enforcement Authorities' Legal Digital Evidence Gathering: Legal, Integrity and Chain-of-Custody Requirement," *Proc. - 2013 Eur. Intell. Secure. Informatics Conf. EISIC 2013*, pp. 198–203, 2013, doi: 10.1109/eisic.2013.44.

[28] A. K. Mishra, M. C. Govil, E. S. Pilli, and A. Bijalwan, "Digital Forensic Investigation of Healthcare Data in Cloud Computing Environment," *J. Healthc. Eng.*, vol. 2022, pp. 1–11, 2022, doi: 10.1155/2022/9709101.

[29] D. Servos and M. Bauer, "Incorporating Off-Line Attribute Delegation into Hierarchical Group and Attribute-Based Access Control," 2020.

[30] B. Leander, A. Causevic, H. Hansson, and T. Lindstrom, "Toward an Ideal Access Control Strategy for Industry 4.0 Manufacturing Systems," *IEEE Access*, vol. 9, pp. 114037–114050, 2021, doi: 10.1109/access.2021.3104649.

[31] G. Liu, W. Pei, Y. Tian, C. Liu, and S. Li, "A novel conflict detection method for ABAC security policies," *J. Ind. Inf. Integr.*, vol. 22, no. 2, p. 100200, 2021, doi: 10.1016/j.jii.2021.100200.

[32] R. Thion, "Access Control Models," in *Cyber Warfare and Cyber Terorism*, IGI Global, 2008.