Unified Access Management for Digital Evidence Storage: Integrating Attribute-based and Role-based Access Control with XACML

Ayu Maulina[1], Zulfany Erlisa Rasjid[2]
Computer Science Program, BINUS Graduate Program
Master of Computer Science Bina Nusantara University, Jakarta, Indonesia 114801[1]
Computer Science Department, School of Computer Science
Bina Nusantara University, Jakarta, Indonesia 11480[2]

Abstract—**Digital evidence is stored in digital evidence storage. An access control system is crucial in situations where not all users can access digital evidence, ensuring that each user's access is limited to what is essential for them to do their jobs. As a result, access control must be included. Role-based access control (RBAC) and attribute-based access control (ABAC) are two of the several varieties of access control. Only the ABAC model is applied in digital evidence storage systems in the research that has been done. In order to get more precise findings, some academics have suggested combining these two models. In light of this, this study suggests a hybrid paradigm for digital evidence storage that combines the key components of both ABAC and RBAC. In addition to utilizing eXtensible Access Control Markup (XACML) throughout the policy statement creation process. A programming language called XACML uses the XML format to specify RBAC and ABAC rules. The study's findings demonstrate that the ABAC and RBAC models can function in accordance with the developed permit and deny test scenarios.**

Keywords*—*ABAC; RBAC; digital evidence storage; XACML; network security

I. Introduction

It can no longer be denied that in this increasingly complex digital era, information and communication technology can no longer be separated from everyday life. However, the increasingly rapid development of this technology also provides great opportunities for cybercrime [1]. Cybercrime itself is a crime that can only be committed via computers, computer networks or other information [2]. Data from the e-MP Robinopsnal Bareskrim Polri shows that the police took action against 8,831 cybercrime cases from January 1 to December 22, 2022. This shows that the level of cybercrime is classified as a serious crime.

Efforts to uncover cybercrime are carried out through a digital investigation process [3] Collecting, storing, and processing digital evidence is part of the investigation and law enforcement process. Existing digital evidence (in the form of text messages, emails, and video recordings) is stored in a storage called digital evidence storage (DES) [4] [5] [6]. One special security measure is to make settings in the access rights section [7]. Every user cannot access digital evidence, so an access management system is needed to ensure that each user only has access appropriate to their duties and responsibilities. Therefore, it is necessary to add access control. Access control is a critical aspect of digital evidence storage systems, determining the security and efficiency of managing access rights. Conventional access control solutions like discretionary access control (DAC) and identity-based access control (IBAC) are inappropriate for use in systems with a substantial user base and unidentified identities. Alternatively, there is a requirement for more sophisticated access control systems [8] [9].

Over the years, various access control models have been explored, such as Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC). ABAC provides a finer degree of control by dynamically determining access rights based on attributes, such as title, location, user identification, and contextual information [10] [11] [12]. While RBAC lowers the danger of illegal access by allowing administrators to assign roles and rights to users and devices in accordance with their responsibilities [10]. In a study conducted by [6] on the ABAC model in digital evidence storage, the findings highlighted the successful performance of the implemented ABAC design. Notably, Panende's comparison between ABAC and RBAC in digital evidence storage demonstrated the superior flexibility of ABAC, making it more suitable for application, although with acknowledged complexities in management and review tasks [6].

Further exploration of ABAC and RBAC reveals that each model possesses distinct strengths and weaknesses. RBAC is recognized for its simplicity in management and review. In contrast, ABAC is deemed more scalable and dynamic due to its ability to capture contextual information for diverse devices and environmental conditions [13] [14]. Both RBAC and ABAC have their own advantages and disadvantages in big corporate applications. Therefore, there is a requirement for a hybrid access control model that combines the strengths of both models [15] [16].

In the context of Indonesia's current access control practices, ABAC is predominantly employed for digital evidence storage. A study by Panende [6] contributed to developing an enhanced ABAC model, addressing the limitations of a simplistic access control system. However, there is a need to improve security and access management systems in the context of digital evidence storage. One of the shortcomings identified is that the approach used is based only on the attributes of the subject, without considering the role that the subject may have in the context of digital evidence storage. In the real world, subjects involved in storing digital evidence have their own roles and responsibilities that need to be considered in access arrangements to ensure data security and integrity. Therefore, to further enhance the security and access management system, this research aims to introduce a novel approach by integrating both ABAC and RBAC models. In [15] hybrid model offers a starting point, but its applicability to digital evidence storage, with a specific emphasis on policy statement clarity, remains unexplored.

This research proposes to utilize the hybrid ABAC and RBAC model in digital evidence storage, employing the eXtensible Access Control Markup Language (XACML) as the policy statement. By combining ABAC's attribute flexibility with RBAC's efficient role management, our objective is to establish a robust access control system that aligns with organizational needs, thereby providing ease for relevant managers in handling access rights security in digital evidence storage. This study addresses the gap in current research by comprehensively examining the hybrid model's implementation and its impact on security and access management within the unique context of digital evidence storage.

II. Related Work

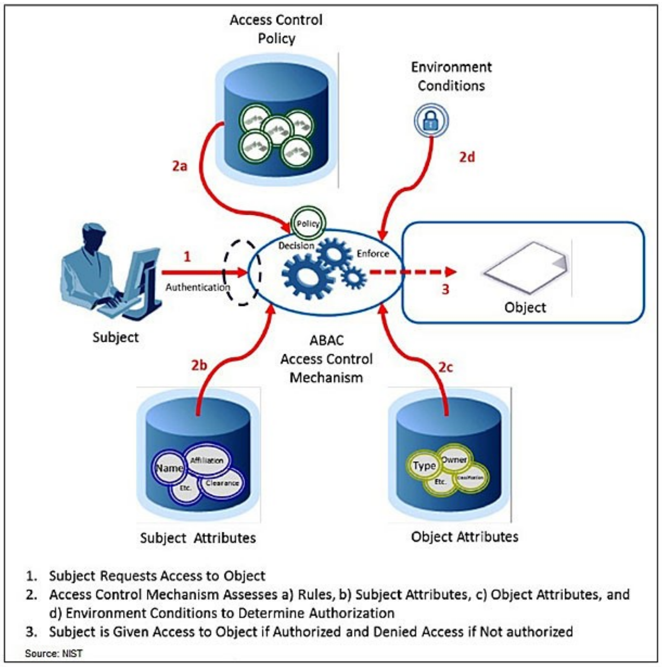
A. Role-Based Access Control (RBAC)

As outlined in the influential 1995 [17], role engineering aims to produce a Role-Based Access Control (RBAC) model. This model assigns permits to access restricted resources to groups of employees who hold the same function within the organisation rather than to individuals. The benefit of using such a model is that it enhances the manageability and flexibility of security administration in organizations with a substantial number of people, resources, and permissions [18]. Over the last three decades, role-based access control (RBAC) has emerged as the de facto access control standard for most businesses [19]. "Least Privilege" and "Segregation of Duties" are the two system security concepts included in the RBAC paradigm [20].

B. Attribute-Based Access Control (ABAC)

ABAC is a method of controlling access to a system based on evaluating attributes associated with the subject, object, requested operations, and sometimes environmental conditions. This evaluation is done by comparing these attributes to policies, rules, or relationships that define the allowed operations for a specific set of attributes. In addition, ABAC allows object owners or administrators to implement access control policies without knowing the exact details of the subject and for an unlimited number of subjects that may need access [21]. As other subjects are incorporated into the organization, there is no requirement to alter the rules and objectives. If the subject is given the requisite characteristics to access the relevant objects, such as assigning those attributes to all Nurse Practitioners in the Cardiology Department, there is no need to make any changes to current rules or object attributes. This advantage is commonly known as accommodating the external (unforeseen) user and is one of the main advantages of implementing ABAC [22].

Fig. 1 depicts a scenario of ABAC access control, illustrating the subject's request for access authorization to the object through several access control mechanisms. This mechanism will gather data in the form of rules, subject attributes, object attributes, and environment attributes. It will grant permission if all requirements are satisfied and deny permission if the conditions are not suitable.



1. Subject Requests Access to Object
2. Access Control Mechanism Assesses a) Rules, b) Subject Attributes, c) Object Attributes, and d) Environment Conditions to Determine Authorization
3. Subject is Given Access to Object if Authorized and Denied Access if Not authorized

Source: NIST

Fig. 1. Basic ABAC Scenario [23].

C. eXtensible Access Control Markup (XACML)

The OASIS, also known as the Organisation for the Advancement of Structured Information Standards, XACML, short for eXtensible Access Control Markup vocabulary, is a universally applicable standard that establishes a vocabulary for composing rules and requests, as well as an architecture, process, and methodology for assessing requests against policies. XACML may be utilized by several access control approaches, including ABAC (Attribute Based Access Control) and RBAC (Role Based Access Control) [24].

XACML consists of several components, including Policy Decision Point (PDP), Policy Administration Point (PAP), Policy Information Point (PIP), and Policy Enforcement Point (PEP). The determination of whether access is allowed or forbidden must be made by the PDP. The PAP is responsible for creating and managing policies, which are kept in the PRP. The PIP must give any additional information required to make access choices. The PEP is responsible for implementing and ensuring compliance with PDP decisions related to access control. XACML is a crucial tool for enterprises and organizations seeking to ensure the security of their networks and data [25]. Fig. 2 provides a concise representation of the XACML concept.

There are several studies that have been carried out related to ABAC, RBAC or XACML. Where [6] on research regarding the application of ABAC to digital storage cabinets and using XACML as a tester for the policies that have been created.

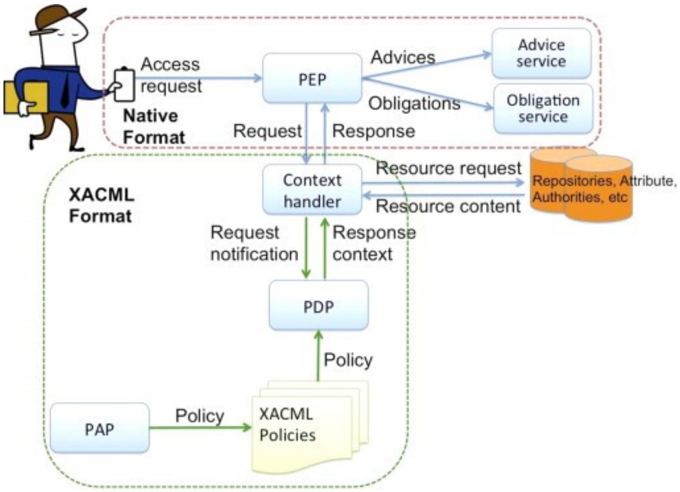


Fig. 2. XACML Overview [26].

Evaluation is carried out by carrying out functional testing, where several scenarios are created and tested with permit or deny conditions according to the scenarios that have been created. The test results show that the ABAC that has been designed can run well according to the existing scenario. Apart from that, several criteria were also compared with the authentication system before and after implementing ABAC, which of course is safer using ABAC. Building on this foundation then [6] also conducted research regarding the comparison between the use of ABAC and RBAC models in digital evidence storage which found that the ABAC model was more suitable to be applied due to its higher level of flexibility.

Furthermore, the ABAC model is also applied in several studies such as that carried out by [9], where he applies the ABAC model and also uses blockchain for security in IoT. Evaluation is carried out by looking at the storage and computation overhead values. Similarly, [27] also used the ABAC model in his research on building a flexible model structure for privacy protection called Attribute-based Access control mechanism for privacy protection in Cloud Systems. Policies are defined in XML form so that administrators can easily determine policies according to their needs. Evaluation is carried out by comparing the performance of the proposed privacy-aware access control with traditional access control models. The results show that the proposed model is successfully implemented, and the processing time difference between the two models is insignificant and acceptable.

Expanding the spectrum of investigations, [28] conducted research validation statements in digital evidence storage and were explored by using first applicable algorithms. The access control model used is ABAC. The evaluation carried out was looking at the analysis of the policy statement and testing the policy statement and the results were that the policy statement was successfully tested and no inconsistencies and incompleteness were found. In the same year [29] also conducted research on digital evidence storage using blockchain for security. Evaluation is carried out by looking at the performance of Block_DEF through simulation experiments. Additionally, [30] conducted research on a combination of models, namely, Attributed-Based Communication Control (ABCC), which focuses on securing communications and data flows in IoT and allows users to determine privacy policies using attributes from various entities.

In a groundbreaking study [15] uses a hybrid method, namely the EGRBAC (RBAC) and HABAC (ABAC) models in smart home IoT. Where the research combines two methods based on role-centric and attribute-centric approaches in model building which produces HyBACRC and HyBACAC. Evaluation is carried out by comparing two aspects, the first is measured through average time processing, which shows that the HyBACAC average processing time value is always lower than the HyBACRC average processing time value. The second comparison was carried out by comparing theoretically, namely basic criteria and quality criteria. More recently [25]conducted research using the RSA-based role-based access control (RBAC) with XACML model in cloud security. In the research, the combination of these models aims to increase privacy and secure communication. In this research, several things are compared, one of which is comparing factors such as scalability, flexibility, privileges and authorization.

Based on an analysis of existing research, it can be inferred that the primary focus in the field of information security is on studying access control models, which may involve the use of ABAC, RBAC techniques, or a mix of both. Nevertheless, the existing body of literature on digital evidence preservation remains rather scarce. Previous studies have examined the use of these models in broad contexts. Still, there is a lack of specific information about the storage of digital evidence, indicating a gap in knowledge. Hence, it is imperative to do more study in the realm of digital evidence preservation, employing the ABAC and RBAC model methodologies. The selection of RBAC is acknowledged for its ease in administration and evaluation, whereas ABAC will be more extensively employed in terms of implementing characteristics to users. The selection was made to address the requirement for straightforward and comprehensible management of RBAC, while also allowing for further customization by assigning attributes to users. This ensures strong access control and meets the needs of diverse digital evidence preservation.

III. Research Methodology

A. Research Flowchart

Fig. 3 shows the research process to be carried out. The stage begins with designing the ABAC and RBAC models in the DES that will be created. After the model has been designed, the next stage is creating a policy statement to determine the applicable rules. This policy statement is made in XACML form, which will produce a file in .xml form, which will then be implemented in the DES system using the Python programming language. After communicating, the next step is to create a simulation as a case scenario consisting of permission and rejection scenarios. After the scenario has been created, the next stage is to test the system by following the scenario. After all the conditions of the case scenario have been completed, the final stage is to evaluate the system that has been created.

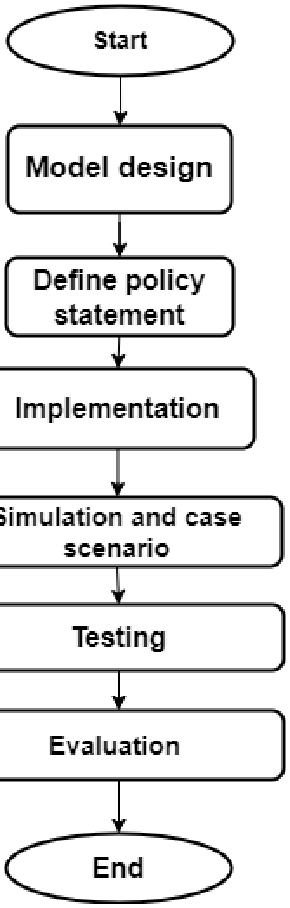


Fig. 3. System flowchart.

B. Model Design

Fig. 4 explains the flow of access control in digital evidence storage systems. The process begins with an actor carrying out the login process by entering a username and password, then the system will carry out an authentication process to check whether the username and password entered are the identities of users who have registered with the system. If the username and password entered are already stored in the system, the next thing to do is check the role and attributes of the user. Checks are carried out to see whether what the user is doing is in accordance with the policies that have been created. Building upon prior research that relied solely on subject, resource, action, and environment checks as the foundation of ABAC, this study introduces advancements in policy verification. Here, an additional layer of checks is applied to user roles. Role-based checks introduce an extra dimension to access management, facilitating the identification and assignment of access privileges based on the user's roles. By incorporating role-based checks, the system ensures that the granted access aligns with the roles assigned to each user. This broadens the scope of access control and provides greater flexibility in determining user permissions, encompassing additional or specific authorizations associated with their roles. Thus, in this research, the checks include the conformity of roles and attributes based on subject, action, resource, and environment which is a combination of both ABAC and RBAC approaches. Suppose the user identification meets the requirements of the policy that has been set. In that case, the action taken is to grant permission to the user so that the user can access the digital evidence storage system. Conversely, if the conditions are unmet, access will be denied. This rejection can occur because the username and password entered are not registered in the system. Second, suppose the policy requirements regarding one of the attributes cannot be met during the verification process. In that case, the result is rejection in the login process, and the user is not permitted to enter the digital evidence storage system.

C. Define Policy Statement

Creating policy statements is an important part of creating access control. Identifying access needs, determining relevant attributes, and formulating policies using XACML format is the main focus in this process. At this stage, we will describe the users involved in this research, consisting of several roles and attributes attached to each user.

D. Implementation

These steps involve establishing an attribute- and role-based access control model for the digital evidence storage system based on the previous design plan. The goal is to ensure that access control implementation runs as desired. Implementation of existing policies will be implemented using the Python programming language. This implementation will later be used to see whether the access control data that has been created can run according to existing rules.

E. Simulation and Case Scenario

The case simulation step involves creating scenarios to test the conformance between access control requirements and system functionality. This case simulation designs access control implementation in a digital evidence storage system. In this case scenario, it will be created in two conditions, namely a permit condition and a deny condition.

This case scenario was created to be used later in the testing stage of the access control that has been created, namely how to adjust the access control needs and the DES system needs. The case scenario that will be created consists of scenarios for permission and rejection. 7 users are described as actors, namely first responder (head), first responder (member), investigator (head), investigator (member), officer (head), officer (member), lawyer. Where each user has their own access rights to DES. Table I table explains the scenarios of permit cases.

TABLE I. PERMIT SIMULATION SCENARIO

User	Role	Subject	Resource	Action	Environtment
First responder (head)	✓	✓	✓	✓	✓
First responder (member)	✓	✓	✓	✓	✓
Investigator (head)	✓	✓	✓	✓	✓
Investigator (member)	✓	✓	✓	✓	✓
Officer (head)	✓	✓	✓	✓	✓
Officer (member)	✓	✓	✓	✓	✓
Lawyer	✓	✓	✓	✓	✓

In simulation case 1, when the user has a role or position as first responder (head), first responder (member), investigator (head), investigator (member), officer (head), officer (member),

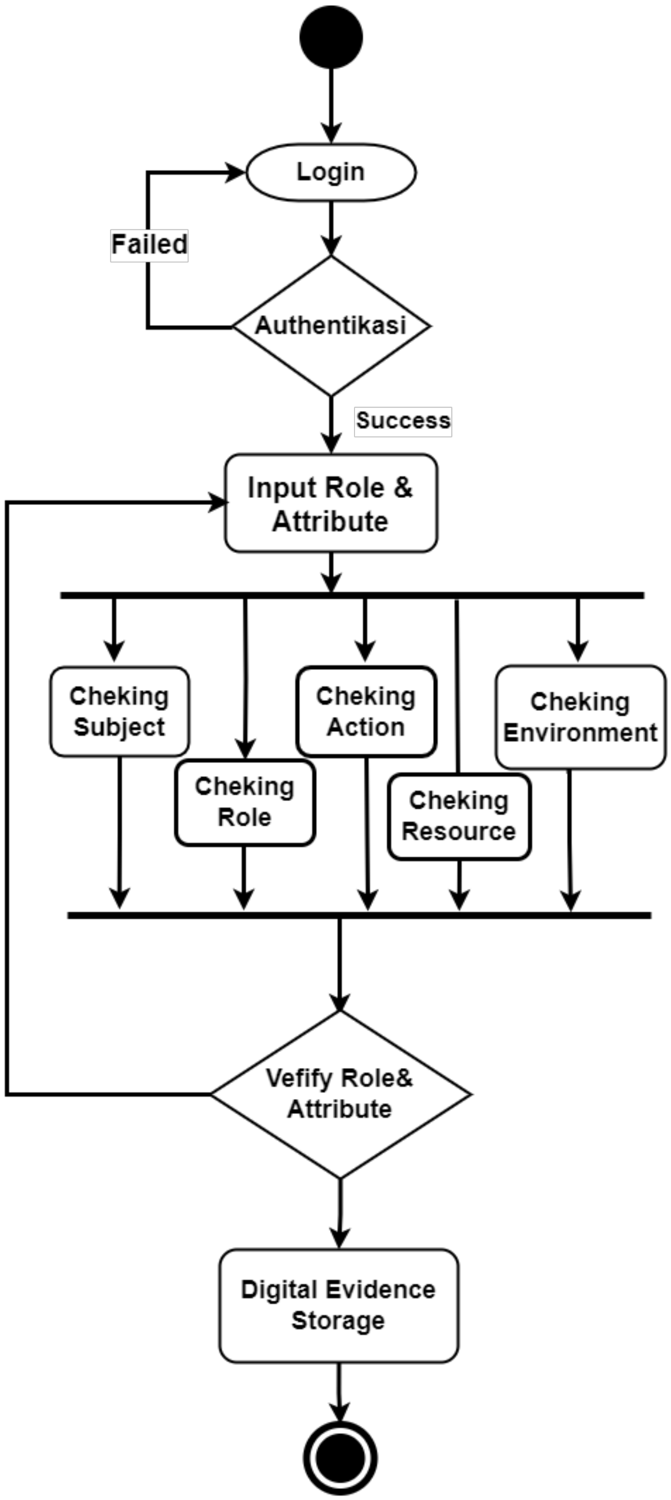


Fig. 4. Access control flow in DES.

lawyer and the access request submitted in accordance with the policies that have been implemented in access control through the role, subject, resource, action and environment elements, the result given is permission. This means the user can access resources or perform requested actions according to his role by complying with all the rules defined in the access policy. Next, Table II will display the scenario of the denied case.

TABLE II. DENY SIMULATION SCENARIO

User	Role	Subject	Resource	Action	Environtment
First responder (head)	✓	-	✓	-	✓
First responder (member)	✓	✓	-	✓	✓
Investigator (head)	✓	✓	✓	-	-
Investigator (member)	✓	-	-	✓	✓
Officer (head)	✓	✓	-	✓	✓
Officer (member)	✓	-	✓	✓	-
Lawyer	✓	✓	✓	-	✓

In the denial case simulation, when the user has the role of first responder (head), first responder (member), investigator (head), investigator (member), officer (head), officer (member), lawyer, but the access request submitted is not fulfills one or more requirements set out in the access policy through the role, subject, resource, action, or environment elements, then the result given is denial. In other words, the user is not permitted to access the resource or perform the requested action because it does not comply with the rules in the applicable access policy.

F. Testing

The testing phase is a crucial component of the design and implementation process, as it attempts to validate that the access control mechanism operates in accordance with the planned design. The output generated during the design stage will be thoroughly evaluated to verify its appropriateness and practicality for keeping digital evidence in the cabinet. The conducted testing include functionality testing to assess the functional performance of the developed model. This testing phase verifies that the implementation of Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC) is functioning correctly according to the defined requirements. This aids in guaranteeing that the system appropriately accesses resources in accordance with predetermined regulations. The objective is to enhance the security of the digital evidence storage system, preventing illegal access.

G. Evaluation

The outcomes of the conducted tests will be evaluated. This level involves the analysis and declaration of access control as having successfully passed the test. The verification of access control is determined by examining the results of system activity testing. In addition, several analyses or assessments will be conducted to compare the criteria necessary for allowing user access. The criteria required when granting access will be compared with previous research conducted by [6].

IV. RESULT

A. Statement Policy

The policy statement in this research involves several subjects with specific roles and responsibilities within the Digital Evidence System (DES). The identified subjects include the following:

1) First Responder: The First Responder is tasked with processing the scene to identify evidence, acquire electronic evidence, and upload digital evidence to

the Digital Evidence System (DES). Here, First Responders are divided into two roles, namely head and member.

2) Investigator: The Examiner is responsible for processing digital evidence within the DES. Investigators are divided in two roles, namely head and member.
3) Officer: The Officer holds the responsibility for overall management within the DES. Officers are divided in two roles, namely head and member.
4) Lawyer: A lawyer is someone who provides advice and defense for others in matters related to the resolution of a legal case. Here, a lawyer is only authorized to download the chain of custody (CoC) form.

The research's policy statements follow the model of the DES policy statements created by Panende [6]. Roles, which are the essential elements of the RBAC paradigm, are an extra feature included here. The table displays the DES policy statement that was suggested in this study.

The Table III illustrates a framework of access control rules that establish permissions and obligations for pertinent entities in the realm of digital evidence storage management. These rules establish the roles, subjects, resources, activities, and environment linked to each entity, serving as the basis for effectively managing and safeguarding digital evidence based on their individual functions. In a policy statement for the Digital Evidence System (DES), there are three roles assigned to the subject entities: head,member, and lawyer. These roles encompass users in the positions of first responder, investigator, officer, and lawyer, where each role is considered an element of the subject. The system involves 15 types of resources serving as objects, nine distinct actions, and three types of environmental conditions reflecting the context in which the requests are initiated.

This policy statement is crafted in the form of XACML (eXtensible Access Control Markup Language). The policy statement is interpreted within the framework of XACML, which is manifested in the form of an XML file. XACML provides a standardized format for expressing access control policies, and in this context, the rules outlined in the statement are represented in XML format as access control policies within the Digital Evidence System (DES).

Through the utilization of XACML and XML representation, this policy statement establishes a structured set of rules for managing access to digital evidence within DES. The resulting XML file serves as a comprehensive guide that can be interpreted by the system to control access and security aspects related to the management of digital evidence.

B. Testing

The access control policy setting in XACML format is dynamically implemented using Python to execute a series of tests on the resulting XML file. The purpose of this test is to evaluate the reliability of the implementation of access control rules based on the previously specified scenarios. The results of the test are displayed in the Table IV.

In the testing permit results, Table IV, it is evident that each input value conforms to the specifications outlined in the established policy statements. Across each row of the table, the combinations of subjects, roles, resources, actions, and environments align with the directives stipulated in the security policy. Consequently, the test outcomes signify that the input values adhere to and comply with the predefined policy statements, resulting in the issuance of permits in accordance with the applicable rules. This conformity reflects the alignment between the provided inputs in each scenario and the implemented access control policies, affirming the system's adherence to the prevailing regulations.

The system utilizes a Python script to read and execute the rules specified in the access control policy XML file. The purpose of these tests is to encompass a range of situations that may occur in digital evidence management, guaranteeing that system responses adhere to defined standards.

The denial scenario testing table, labeled as V, clearly demonstrates that specific input values vary from the stated policy standards, resulting in the denial of access. Every test scenario corresponds to a distinct combination of people, roles, resources, activities, and environments, accompanied by their own IP addresses, MAC addresses, and temporal access limitations. Each of these test situations demonstrates that the "Deny" decision signifies a departure from the defined policy declarations, resulting in the refusal of access. The disparities are emphasized in bold language, denoting input values that do not conform to the predetermined norms. This scholarly depiction emphasizes the occurrences when mistakes were made, shown by the refusal of entry in accordance with the infractions of the rules.

V. Discussion

Based on the results of the permit (permit) and denial (deny) tests, it can be concluded that the access control that has been built complies with the established rules. In addition, it can be revealed that the access control shows a good level of consistency and completeness. Consistency is defined as unfairness where there are two rules that produce conflicting results. In this context, each rule is represented by three elements, namely subject (S), object (O), and action (A), with the decision (D) in the form of three tuples (s, o, a) $\rightarrow$ d. It is said that a policy suffers from inconsistency if two rules, and , that satisfy certain conditions, produce conflicting decisions. In this study, no inconsistencies were found in the policy statement for the Digital Evidence System (DES) after testing. The policy statement has been prepared in accordance with existing regulations.

Meanwhile, incompleteness is a condition where there are rules that have not been included in a predefined set of rules. This means there is a rule (r) for a condition where r $\notin$ R (r is not included in R, which is the set of rules established beforehand). For example, in this study's incompleteness, we can specify that the **first responder** subject should have 5 rules. However, in the preparation, only 4 rules have been established, leaving 1 rule not included in the set of rules for the **first responder** subject. In other words, there is a lack of rules that need to be established to cover all necessary aspects in access rights management for this subject. However, no incompleteness was found in this study based on the conducted testing.

TABLE III. POLICY STATEMENT

	Subject	Role	Resources	Actions	Environment
Rule	First Responder	Head	Upload digital evidence	Upload	Ip address Mac address Time access
			Create rack	Create	
			Create Cabinet	Create	
			Create bag	Create	
			Input data case coc	Input	
		Member	Upload digital evidence	Upload	
			Create bag	Create	
			Input data case coc	Input	
	Investigator	Head	Download Digital Evidence	Download	Ip address Mac address Time access
			Complete the Data Coc	Complete	
			Validate data coc	Validate	
		Member	Download Digital Evidence	Download	
			Complete the Data Coc	Complete	
	Officer	Head	Delete Digital Evidence	Delete	Ip address Mac address Time access
			Change Password User	Change password	
			Change Code Signature	Change code	
			Download Form Coc	Download Form	
			Validate Digital Evidence	Validate	
			Validate Case Status	Validate	
			Validate Data Coc	Validate	
		Member	Delete Digital Evidence	Delete	
			Change Password UUser	Change Password	
			Download Form Coc	Download	
	Lawyer	Lawyer	Download Form Coc	Download Form	Ip address Mac address Time access

TABLE IV. TESTING RESULT OF PERMIT SCENARIO

Testing to scenario	Subject	Role	Resource	Actions	Environment	Test Result
1	First Responder	Head	Upload Digital Evidence	Upload	IP Addres : 202.58.180.194 MAC Address : 9E:3D:7A:F5:EB:D6 Time Access : 00:00-23:59	Permit
2	First Responder	Member	Create Bag	Create	IP Address : 202.58.180.194 MAC Address : 9E:3D:7A:F5:EB:D6 Time Access : 00:00-23:59	Permit
3	Investigator	Head	Complete the Data Coc	Complete Data	IP Addres : 202.58.180.194 MAC Address : 9E:3D:7A:F5:EB:D6 Time Access : 00:00-23:59	Permit
4	Investigator	Member	Download Digital Evidence	Download	IP Address : 202.58.180.194 MAC Address : 9E:3D:7A:F5:EB:D6 Time Access : 00:00-23:59	Pemit
5	Officer	Head	Delete Digital Evidence	Delete	IP Address : 202.58.180.194 MAC Address : 9E:3D:7A:F5:EB:D6 Time Access : 00:00-23:59	Permit
7	Officer	Member	Change Password User	Change Password	IP Address : 202.58.180.194 MAC Address : 9E:3D:7A:F5:EB:D6 Time Access : 00:00-23:59	Permit
8	Lawyer	Lawyer	Download Form Coc	Download Form	IP Address : 202.58.180.194 MAC Address : 9E:3D:7A:F5:EB:D6 Time Access : 00:09-15:00	Permit

In addition to the aforementioned components, it is important to highlight that system testing include the assessment of the performance of the constructed access control. The duration of each test is used as a measure to assess the effectiveness and promptness of the system. The results of the time required for checking can be seen in the Table VI.

Table VI documents the recorded times for access control in permit and deny scenarios during testing. In the analytical context, the average testing time across all scenarios is considered as a metric to reflect the overall performance of the access control. It is important to note that this average encompasses the entire testing period without distinguishing between permit and deny scenarios. Consequently, these results depict a comprehensive view of the efficiency of the access control system without specifically assessing the differences between permit and deny scenarios. The presentation of this overall average provides a holistic perspective on the overall responsiveness of the access control system.

Based on the reported findings, it can be inferred that the constructed access control system demonstrates optimal performance in terms of both time and consistency. The access control in this system can be regarded as more robust than the access control in the preceding Digital Evidence System (DES), particularly in terms of the quantity of elements taken into account during the verification process. Table VII provides a comparison of access control features between the present implementation and the old DES. In evaluating the findings of this research, it is important to note that the primary focus on the aspects of time and accuracy in the implementation of the new access control system demonstrates substantial sufficiency

TABLE V. Testing Result of Deny Scenario

Testing to scenario	Subject	Role	Resource	Actions	Environment	Test Result
1	**Investigator**	Head	Upload Digital Evidence	**Download**	IP Addres : 202.58.180.194 MAC Address : 9E:3D:7A:F5:EB:D6 Time Access : 00:00-23:59	Deny
2	First Responder	Member	**Create Cabinet**	Create	IP Address : 202.58.180.194 MAC Address : 9E:3D:7A:F5:EB:D6 Time Access : 00:00-23:59	Deny
3	Investigator	Head	Validate Data Coc	**Complete Data**	**IP Addres : 223.255.229.74** MAC Address : 9E:3D:7A:F5:EB:D6 Time Access : 00:00-23:59	Deny
4	**First Responder**	Member	**Create Bag**	Download	IP Address : 202.58.180.194 MAC Address : 9E:3D:7A:F5:EB:D6 Time Access : 00:00-23:59	Deny
5	Officer	Head	**Input Data Case Coc**	Validate	IP Address : 202.58.180.194 MAC Address : 9E:3D:7A:F5:EB:D6 Time Access : 00:00-23:59	Deny
7	**Lawyer**	Member	Delete Digital Evidence	Delete	**IP Address : 223.255.229.74** MAC Address : 9E:3D:7A:F5:EB:D6 Time Access : 00:00-23:59	Deny
8	Lawyer	Lawyer	Download Form Coc	**Upload**	IP Address : 202.58.180.194 MAC Address : 9E:3D:7A:F5:EB:D6 Time Access : 00:09-15:00	Deny

TABLE VI. Time Testing

Time Testing of Permit Scenario (ms)	Time Testing of Deny Scenario
0.0000009	0.0000007
0.0000004	0.0000005
0.0000014	0.0000005
0.0000005	0.0000006
0.0000016	0.0000006
0.0000005	0.000002
0.0000018	0.0000006
Average time : 0,0000009	

in performance enhancement. Considering the outcomes derived from both approaches, it is evidenced that the proposed system has attained a high level of efficiency with significant execution time and satisfactory accuracy levels in user access verification. Therefore, direct comparison with the previous system is deemed irrelevant in the context of this performance enhancement, as the superior implementation has successfully achieved the research goal of faster and more precise access control.

TABLE VII. Comparison Method

Component	Access Control	
	ABAC	**ABAC & RBAC**
Username	✓	✓
Password	✓	✓
Authentication	✓	✓
Authorization	✓	✓
Rule Policy	✓	✓
Attribute Subject	✓	✓
Attribute Resource	✓	✓
Attribute Action	✓	✓
Attribute Environment	✓	✓
Role	x	✓

The primary objective of this research is to enhance system security through the development of more resilient access control mechanisms. The addition of the Role-Based Access Control (RBAC) feature to the model, which was initially based on Attribute-Based Access Control (ABAC), enables this achievement. This modification aims to enhance the verification functionality by incorporating a novel aspect in the form of user roles in the determination of access privileges. The RBAC feature aims to enhance access control by enabling it to be more agile and adaptable to changes in the system environment. This update is designed to bolster system security, particularly in the area of user access control, in order to provide a heightened level of protection for the system's resources and data.

VI. Conclusion

In this research, combining Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) through the application of the XACML policy language to digital evidence storage has shown good results. The main objective of this research is to increase the level of robustness of access control, with the aim that the system is able to carry out policy statements in accordance with predetermined provisions.

Research findings show that the integration of RBAC and ABAC using the XACML policy language is able to provide consistent and comprehensive access control. The addition of the role feature in the access checking process provides an additional dimension in ensuring system security, which substantially strengthens access control and contributes positively to overall system performance. In addition, the time required to check access in this system is relatively small, bringing positive impact on the efficiency of the system verification process. Overall, the results of this study imply that the incorporation of RBAC and ABAC via XACML in digital evidence storage can be considered as a significant step towards more efficient and robust access control within an information security framework.

However, to continue this research, a security evaluation against specific attacks is necessary. Further research can explore how this model can maintain security in the face of targeted attacks, such as policy injection attacks or attacks on digital evidence storage. Security enhancement may involve the development of effective detection and protection mechanisms to address potential threats targeted at the system.

References

[1] N. K. N. Widiasari and E. F. Thalib, "The impact of information technology development on cybercrime rate in indonesia," *Journal of Digital Law and Policy*, vol. 1, no. 2, pp. 73–86, 2022.

[2] R. Baranenko, "Cyber crime, computer crime or cyber offense? the analysis of the features of a terminology application," *National Technical University of Ukraine Journal. Political science. Sociology. Law*, 2021.

[3] D.-Y. Kao, Y.-T. Chao, F. Tsai, and C.-Y. Huang, "Digital evidence analytics applied in cybercrime investigations," in *2018 IEEE Conference on Application, Information and Network Security (AINS)*, pp. 111–116, 2018.

[4] A. M. Faruq, S. M. Andri, and P. Yudi, "Clustering storage method for digital evidence storage using software defined storage," in *IOP Conference Series: Materials Science and Engineering*, vol. 722, p. 012063, IOP Publishing, 2020.

[5] M. A. Romli, Y. Prayudi, and B. Sugiantoro, "Storage area network architecture to support the flexibility of digital evidence storage," *International Journal of Computer Applications*, vol. 975, p. 8887, 2019.

[6] M. F. Panende, Y. Prayudi, and I. Riadi, "Comparison of attribute based access control (abac) model and rule based access (rbac) to digital evidence storage (des)," *International Journal of Cyber-Security and Digital Forensics*, vol. 7, no. 3, pp. 275–283, 2018.

[7] S. Rana and D. Mishra, "An authenticated access control framework for digital right management system," *Multimedia Tools and Applications*, vol. 80, pp. 25255–25270, 2021.

[8] L. Malina, P. Muzikant, M. Nohava, J. Hajny, A. Dufka, P. Svenda, and V. Stupka, "Secure cloud storage system for digital evidence," in *2023 15th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pp. 134–139, IEEE, 2023.

[9] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for iot," *IEEE Access*, vol. 7, pp. 38431–38441, 2019.

[10] M. Bhargavi and Y. Pachipala, "Enhancing iot security and privacy with claims-based identity management," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 11, 2023.

[11] V. C. Hu, D. Ferraiolo, R. Kuhn, A. R. Friedman, A. J. Lang, M. M. Cogdell, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone, *et al.*, "Guide to attribute based access control (abac) definition and considerations (draft)," *NIST special publication*, vol. 800, no. 162, pp. 1–54, 2013.

[12] G. Sahani, C. S. Thaker, and S. M. Shah, "Supervised learning-based approach mining abac rules from existing rbac enabled systems," *EAI Endorsed Trans. Scalable Inf. Syst.*, vol. 10, p. e9, 2022.

[13] M. umar Aftab, Z. Qin, S. Ali, J. Khan, *et al.*, "The evaluation and comparative analysis of role based access control and attribute based access control model," in *2018 15th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, pp. 35–39, IEEE, 2018.

[14] B. Bezawada, K. Haefner, and I. Ray, "Securing home iot environments with attribute-based access control," in *Proceedings of the Third ACM Workshop on Attribute-Based Access Control*, pp. 43–53, 2018.

[15] S. Ameer, J. Benson, *et al.*, "Hybrid approaches (abac and rbac) toward secure access control in smart home iot," *IEEE Transactions on Dependable and Secure Computing*, 2022.

[16] S. Long and L. Yan, "Racac: An approach toward rbac and abac combining access control," in *2019 IEEE 5th International Conference on Computer and Communications (ICCC)*, pp. 1609–1616, IEEE, 2019.

[17] R. S. Sandhu, "Role-based access control," in *Advances in computers*, vol. 46, pp. 237–286, Elsevier, 1998.

[18] C. Blundo, S. Cimato, and L. Siniscalchi, "Managing constraints in role based access control," *IEEE Access*, vol. 8, pp. 140497–140511, 2020.

[19] G. Batra, V. Atluri, J. Vaidya, and S. Sural, "Deploying abac policies using rbac systems," *Journal of computer security*, vol. 27, no. 4, pp. 483–506, 2019.

[20] M. Uddin, S. Islam, and A. Al-Nemrat, "A dynamic access control model using authorising workflow and task-role-based access control," *Ieee Access*, vol. 7, pp. 166676–166689, 2019.

[21] S. Ameer, J. O. Benson, and R. S. Sandhu, "An attribute-based approach toward a secured smart-home iot access control and a comparison with a role-based approach," *Inf.*, vol. 13, p. 60, 2022.

[22] V. C. Hu, D. F. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, "Guide to attribute based access control (abac) definition and considerations," 2014.

[23] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone, *et al.*, "Guide to attribute based access control (abac) definition and considerations," *NIST special publication*, vol. 800, no. 162, pp. 1–54, 2014.

[24] Ó. M. Pereira, V. Semenski, D. D. Regateiro, and R. L. Aguiar, "The xacml standard - addressing architectural and security aspects," in *International Conference on Internet of Things, Big Data and Security*, 2017.

[25] A. Kousalya and N.-k. Baik, "Enhance cloud security and effectiveness using improved rsa-based rbac with xacml technique," *International Journal of Intelligent Networks*, vol. 4, pp. 62–67, 2023.

[26] C. D. P. K. Ramli, H. R. Nielson, and F. Nielson, "The logic of xacml," *Science of Computer Programming*, vol. 83, pp. 80–105, 2014.

[27] H. X. Son and N. M. Hoang, "A novel attribute-based access control system for fine-grained privacy protection," in *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, pp. 76–80, 2019.

[28] A. Syauqi, I. Riadi, and Y. Prayudi, "Validation policy statement on the digital evidence storage using first applicable algorithm," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 10, 2019.

[29] Z. Tian, M. Li, M. Qiu, Y. Sun, and S. Su, "Block-def: A secure digital evidence framework using blockchain," *Information Sciences*, vol. 491, pp. 151–165, 2019.

[30] S. Bhatt and R. Sandhu, "Abac-cc: Attribute-based access control and communication control for internet of things," in *Proceedings of the 25th ACM Symposium on Access Control Models and Technologies*, pp. 203–212, 2020.