

Journal Scientific and Applied Research, Vol. 31, 2026
International Journal

ISSN 1314-6289 (Print)
ISSN 2815-4622 (Online)

Original Contribution

SCENARIO-BASED METHODOLOGY FOR EVALUATING A HYBRID ACCESS CONTROL METHOD IN UNIVERSITY INFORMATION SYSTEMS

Radostin H. Lefterov

Department of Mathematics, Informatics and Natural Sciences, Technical University of Gabrovo, Gabrovo, Bulgaria, e-mail: rikitab@gmail.com

Abstract: *This paper presents a scenario-based methodology for evaluating a hybrid access control method intended for university information systems. The proposed approach combines role-based and attribute-based access control with contextual information, SIEM and EDR signals, and dynamic risk assessment. A structured set of ten evaluation scenarios is defined for student, lecturer, and administrative access, including normal conditions, insufficient permissions, changed context, increased risk, and critical security situations. The methodology also defines comparative criteria for examining the expected behaviour of traditional RBAC, RBAC combined with ABAC, and the proposed hybrid method. The presented scenarios do not represent completed experimental results, but provide a consistent basis for subsequent implementation and validation in a controlled university information system environment.*

Key words: *Access Control, Hybrid Method, RBAC, ABAC, Context-Aware Access Control, Risk Assessment, SIEM, EDR, University Information Systems.*

1. Introduction

University information systems integrate a large number of users, resources, and services with different levels of access. Students, lecturers, and administrative staff use the same information environment, but perform different functions and have different access rights. This requires the use of mechanisms capable of restricting access according to the role and specific privileges of each user.

Traditional role-based access control provides a clear and relatively easy-to-manage foundation, but in more dynamic environments this is not always sufficient. Having permission to access a resource does not provide information about the conditions under which the request is made. The same user may access the system from a different network, device, or location, or at a time when signs of suspicious activity have already been detected. For this reason, access decisions should also take into account additional information related to the specific request [1–3].

In a previous stage of the research, a hybrid cybersecurity method intended for application in a university information system was developed. The method combines role-

based and attribute-based access control, contextual information, data from Security Information and Event Management systems, and information from Endpoint Detection and Response systems. The collected information is used to determine the level of risk and to form the final access decision. The approach follows the principle that each request should be evaluated independently and that previously granted privileges should not automatically result in access being allowed [4].

After developing such a method, it is necessary to define an appropriate approach for its subsequent evaluation. For this purpose, predefined scenarios can be used to represent typical situations in the operation of a university information system. By changing the user role, requested resource, operation, contextual conditions, and available security signals, it is possible to examine how the access decision process is expected to change.

The aim of this paper is to develop a scenario-based methodology for evaluating the proposed hybrid access control method in university information systems. The methodology defines user groups, resources, operations, access conditions, and risk factors that can be used in a subsequent experimental study. In addition, evaluation criteria are defined to allow the behaviour of the hybrid method to be compared with role-based access control and with a combined role- and attribute-based approach.

The main contribution of this paper is the definition of a structured scenario-based methodology for the subsequent evaluation of the proposed hybrid access control method. Unlike approaches that examine individual access control mechanisms separately, the proposed methodology considers user roles, attributes, contextual conditions, and security signals within a common evaluation process. The developed scenarios are intended to provide a consistent basis for comparing the expected behaviour of RBAC, RBAC combined with ABAC, and the proposed hybrid method under different access and risk conditions.

2. Related work

Role-Based Access Control is one of the most widely used approaches for managing access in information systems. Its main advantage is the clear assignment of permissions through predefined roles, which makes administration easier in environments with a large number of users. However, RBAC remains relatively static and does not naturally take into account dynamic factors such as time, location, device, or current system conditions. This limits its effectiveness in situations where the context of an access request changes frequently [1].

Attribute-Based Access Control extends this concept by using attributes related to the user, resource, action, and environment. This allows more detailed and flexible access policies to be defined. ABAC can adapt the access decision according to the specific conditions of a request, but this flexibility also increases the complexity of policy definition and management. The effectiveness of the approach strongly depends on the availability of accurate and up-to-date attribute information [2].

Context-aware access control introduces additional dynamic information into the decision-making process. Parameters such as network, device, location, and time can be used to modify the access decision according to the current situation. This approach is particularly suitable for distributed and remote access environments, but its reliability depends on the quality of the collected contextual information. In practice, context-aware mechanisms are often used as an additional security layer rather than as a standalone access control solution [3].

Risk-based access control extends this concept by dynamically estimating the security risk associated with an access request and using it as an additional factor in the authorization decision [5].

Access control mechanisms can also be complemented by security monitoring technologies. Security Information and Event Management systems collect and analyse events from different infrastructure components and can identify suspicious patterns that may not be visible when individual events are considered separately [6]. Endpoint Detection and Response systems provide additional information about the state and behaviour of endpoint devices and support the detection of potentially malicious activity [7]. These technologies do not directly determine access permissions, but the information they provide can be used as an additional input in the evaluation of an access request.

The reviewed approaches address different aspects of cybersecurity and therefore should not be considered mutually exclusive. RBAC provides a stable foundation for access management, ABAC introduces more detailed conditions, context-aware control reflects changes in the environment, while SIEM and EDR provide information about the current security state. This creates the possibility of combining their capabilities within a common access decision process. The hybrid method considered in this paper follows this approach by using several independent sources of information when evaluating a request instead of relying on a single access control mechanism.

3. Proposed Hybrid Access Control Method

The proposed hybrid method is designed as a sequence of interconnected checks performed before a final access decision is made. Its architecture combines user authentication, role management, attribute management, evaluation of access conditions, risk assessment, decision making, monitoring and event registration, as well as incident response. SIEM and EDR components are also included as additional sources of information used during risk evaluation.

After successful authentication, the role of the user is determined and the corresponding basic access rights are identified. These rights form the initial basis for processing the request. Typical roles in a university information system include student, lecturer, doctoral student, administrative employee, and system administrator. The use of roles simplifies access management because permissions are assigned at role level rather than individually for each user.

The initial role-based decision is then refined through additional information. The method considers contextual parameters such as time, network, device, location, access frequency, and unusual user behaviour. None of these parameters is treated as sufficient on its own to deny access. Instead, they are evaluated together with information from the remaining modules and are used as input for the risk assessment process.

The risk assessment module combines the information collected during the previous checks and determines the overall level of risk associated with the request. Three risk levels are used: low, medium, and high. A low level indicates that no significant deviations have been detected, a medium level reflects the presence of factors requiring additional attention, while a high level is associated with several indicators of increased security risk.

The final decision is not limited to a simple grant or deny outcome. Depending on the evaluated risk, the system may grant access, provide restricted access, require additional verification, deny access, notify an administrator, or block the active session. This allows the method to react more flexibly to suspicious conditions instead of treating every deviation as an immediate reason for complete denial.

In the proposed logic, low-risk requests normally lead to access being granted. Medium-risk requests may result in restricted access or additional verification, while high-risk requests may lead to denial, administrator notification, or session blocking. The final decision is

therefore based on a combined assessment of the available information rather than on a single criterion.

4. Scenario-Based Evaluation Methodology

The proposed evaluation methodology is based on predefined access scenarios that represent typical situations in a university information system. The purpose of the methodology is to provide a structured way to examine how the hybrid method is expected to behave under different access conditions and different levels of risk.

Each scenario is defined through a set of parameters describing the user, the requested resource, the operation, and the conditions under which the request is made. The main parameters include the user role, resource type, requested operation, relevant user and resource attributes, contextual conditions, available EDR information, available SIEM information, and the expected risk level. This structure allows the same type of request to be examined under both normal and changed security conditions.

The methodology distinguishes several groups of conditions. Normal conditions represent requests made with valid permissions and without significant deviations from the expected behaviour. Changed contextual conditions may include access outside the usual time interval, the use of an unknown device, connection through an external network, or other deviations from the common access pattern. Suspicious and high-risk conditions are represented through combinations of several contextual factors or through security signals indicating potentially malicious activity.

For each defined scenario, the expected risk level and the expected decision of the hybrid method are specified in advance. This makes it possible to establish a reference behaviour before the actual experimental implementation. The expected decision can be Grant, Additional verification, Restricted access, Deny, or Block, depending on the evaluated combination of access rights, context, and security signals.

The methodology is intended to support a later comparison between three approaches: traditional RBAC, a combined RBAC+ABAC approach, and the proposed hybrid method. The same access request can therefore be evaluated according to the logic of each approach, making it possible to identify situations in which contextual information or additional security signals are expected to influence the final decision.

The scenarios are organized around three main user groups in a university information system: students, lecturers, and administrative users. Additional combined-risk scenarios are included in order to examine situations in which several risk factors occur simultaneously. One of the combined-risk scenarios includes a critical SIEM or EDR signal, allowing the methodology to represent cases in which a high risk level is expected regardless of the existence of valid basic access rights.

For every scenario, the information can be recorded in a structured form containing the scenario identifier, user type, access conditions, expected risk level, and expected decision. This provides a uniform basis for the subsequent experimental stage and for comparison between different access control approaches.

5. Evaluation Scenarios and Comparative Criteria

Based on the proposed methodology, ten evaluation scenarios are defined. They cover normal access, requests without sufficient permissions, changed contextual conditions, and situations involving increased or critical security risk. The scenarios are divided according to the main user groups of the university information system and are presented in Table 1.

Table 1. Proposed evaluation scenarios

ID	User / scenario	Main conditions	Expected risk	Expected decision
S1	Student – access to own grades	Valid permissions, usual time, known device, trusted network, no security alerts	Low	Grant
S2	Student – access to another student's data	No permission for the requested resource, normal contextual conditions	Low	Deny
S3	Student – access under changed contextual conditions	Valid permissions, external network, unknown device, no critical security alert	Medium	Additional verification
S4	Lecturer – access to own course records	Valid permissions, usual time, known device, university network, no security alerts	Low	Grant
S5	Lecturer – access outside assigned permissions	Request for a resource outside the lecturer's assigned courses or responsibilities	Low	Deny
S6	Lecturer – valid access under increased contextual risk	Valid permissions, unusual time, external network, unknown device	Medium	Additional verification / Restricted access
S7	Administrative user – normal access to student records	Valid administrative permissions, known device, normal network and time conditions	Low	Grant
S8	Administrative user – access to sensitive data under increased risk	Valid permissions, external network, unknown device, unusual access conditions	Medium	Additional verification / Restricted access
S9	Combined-risk access request	Valid basic permissions, unusual time, external network, unknown device, suspicious activity detected	High	Deny
S10	Access request with a critical security signal	Valid basic permissions, critical SIEM or EDR signal detected	High	Deny / Block

The scenarios are designed so that the effect of different types of information can be examined separately and in combination. Scenarios S1, S4, and S7 represent normal access conditions, while S2 and S5 verify the effect of insufficient permissions. Scenarios S3, S6, and S8 introduce contextual deviations without a critical security signal. The final two scenarios represent accumulated and critical risk conditions. This structure makes it possible to examine not only whether access should be granted or denied, but also when additional verification or restricted access may be more appropriate.

5.1. Comparative Criteria

The comparison uses RBAC and RBAC+ABAC as baseline access control approaches, while contextual information, SIEM, EDR, and dynamic risk assessment are evaluated as integrated components of the proposed hybrid method.

The same access scenarios can be used to compare the behaviour of three different approaches: traditional RBAC, a combined RBAC+ABAC model, and the proposed hybrid method. The comparison is based on the decision produced for each scenario and on the type of information used during the decision-making process.

The main comparative criteria include whether the request is granted or denied, whether additional verification or restricted access is required, and whether the decision changes when contextual or security-related information is introduced. Particular attention is given to scenarios in which the user has valid basic permissions but the current conditions indicate increased or critical risk.

This comparison is intended to identify situations in which a role-based decision alone is not sufficient and where additional attributes, contextual conditions, or SIEM/EDR signals may influence the final outcome.

The three approaches differ not only in the final access decision, but also in the type of information considered during request evaluation. For this reason, an additional comparison can be made according to the information sources and control mechanisms used by each approach. This comparison does not represent experimental results, but summarizes the functional scope of the evaluated models.

Table 2. Comparison of Information Used by the Evaluated Access Control Approaches

Evaluation factor	RBAC	RBAC + ABAC	Hybrid method
User role	Yes	Yes	Yes
User/resource attributes	No	Yes	Yes
Contextual conditions	No	Yes / policy-dependent	Yes
SIEM information	No	No	Yes
EDR information	No	No	Yes
Dynamic risk level	No	No	Yes
Additional verification / restricted access	Usually no	Policy-dependent	Yes

Table 2 shows that the main difference between the three approaches is the amount and type of information involved in the decision-making process. RBAC relies mainly on predefined roles and permissions, while RBAC+ABAC introduces additional attributes that allow more detailed access policies. The proposed hybrid method extends this logic by also considering contextual conditions, security monitoring information, and a dynamically determined risk level.

This broader evaluation allows the hybrid method to distinguish between requests that have identical basic permissions but are made under different security conditions. As a result, the final decision may include not only access approval or denial, but also additional verification, restricted access, or blocking in higher-risk situations.

6. Discussion

The proposed scenario-based methodology provides a structured way to examine how different access control approaches are expected to react under changing security conditions.

Its main purpose is not to replace experimental validation, but to define a consistent basis for future testing of the proposed hybrid method.

The scenarios show that the largest differences between the evaluated approaches are expected to appear when a user has valid basic permissions, but the request is made under unusual or potentially risky conditions. In such cases, traditional RBAC may still allow access because the role itself has not changed. A combined RBAC+ABAC approach can introduce additional restrictions through attributes and policy conditions, but it does not necessarily include information about the current security state of the system or the endpoint device.

The proposed hybrid method extends the decision process by combining access rights with contextual conditions and security-related information. This is particularly important in scenarios involving an external network, an unknown device, unusual access time, abnormal behaviour, or alerts generated by SIEM or EDR components. These factors may change the risk level even when the user has valid permissions for the requested resource.

Another important aspect of the methodology is that not every deviation leads directly to access denial. Medium-risk situations may result in additional verification or restricted access, while high-risk conditions may lead to denial or session blocking. This provides a more flexible response compared with models in which the outcome is limited mainly to grant or deny.

The proposed methodology also has limitations. At this stage, the scenarios describe expected system behaviour and have not yet been validated through a complete experimental implementation. The actual effect of the individual contextual parameters and security signals will depend on the configuration of the university information system, the available monitoring components, and the selected risk assessment rules. For this reason, the next stage of the research should include practical implementation of the proposed method and execution of the defined scenarios in a controlled environment.

This future experimental stage will make it possible to verify whether the expected decisions correspond to the actual behaviour of the implemented system and to determine in which scenarios the hybrid approach provides a measurable advantage over RBAC and RBAC+ABAC.

7. Conclusion

This paper presents a scenario-based methodology for the evaluation of a hybrid access control method intended for university information systems. The proposed methodology defines a structured set of user roles, resources, operations, contextual conditions, security signals, expected risk levels, and access decisions that can be used as a basis for subsequent experimental validation.

Ten evaluation scenarios were defined to represent normal access, insufficient permissions, changed contextual conditions, increased risk, and critical security situations. The scenarios cover student, lecturer, and administrative access, as well as combined-risk cases involving several security factors. This provides a consistent framework for examining how different types of information may influence the access decision.

The methodology also establishes a basis for comparison between traditional RBAC, RBAC combined with ABAC, and the proposed hybrid method. The main difference of the hybrid approach is the inclusion of contextual information, SIEM and EDR signals, and dynamic risk assessment in the decision-making process. This allows access decisions to go beyond a simple grant-or-deny model and to include additional verification, restricted access, or blocking when required.

At the current stage, the proposed scenarios describe the expected behaviour of the method and do not represent results from completed experiments. The next stage of the

research will focus on the implementation of the hybrid method in a controlled university information system environment and on the execution of the defined scenarios. This will allow the expected decisions to be compared with the actual system behaviour and will provide a basis for evaluating the practical applicability of the proposed approach.

References

[1] Sandhu, R. S., E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control Models," Computer, vol. 29, no. 2, pp. 38–47, 1996. DOI: 10.1109/2.485845.

[2] Hu, V. C., D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, Guide to Attribute Based Access Control (ABAC) Definition and Considerations, NIST Special Publication 800-162, National Institute of Standards and Technology, 2014, updated 2019. DOI: 10.6028/NIST.SP.800-162.

[3] Kayes, A. S. M., R. Kalaria, I. H. Sarker, M. S. Islam, P. A. Watters, A. Ng, M. Hammoudeh, S. Badsha, and I. Kumara, "A Survey of Context-Aware Access Control Mechanisms for Cloud and Fog Networks: Taxonomy and Open Research Issues," Sensors, vol. 20, no. 9, art. 2464, 2020. DOI: 10.3390/s20092464.

[4] Rose, S., O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207, National Institute of Standards and Technology, 2020. DOI: 10.6028/NIST.SP.800-207.

[5] Atlam, H. F., M. A. Azad, M. O. Alassafi, A. A. Alshdadi, and A. Alenezi, "Risk-Based Access Control Model: A Systematic Literature Review," Future Internet, vol. 12, no. 6, art. 103, 2020. DOI: 10.3390/fi12060103.

[6] González-Granadillo, G., S. González-Zarzosa, and R. Diaz, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures," Sensors, vol. 21, no. 14, art. 4759, 2021. DOI: 10.3390/s21144759.

[7] Shen, X., Z. Li, G. Burleigh, L. Wang, and Y. Chen, "Decoding the MITRE Engenuity ATT&CK Enterprise Evaluation: An Analysis of EDR Performance in Real-World Environments," Proceedings of the 19th ACM Asia Conference on Computer and Communications Security (ASIA CCS '24), pp. 96–111, 2024. DOI: 10.1145/3634737.3645012.