Secured Access Control in Security Information and Event Management Systems

Leila Rikhtechi
Department of Computer Engineering, Faculty of Engineering, Arak University, Arak 38156-8-8349, Iran
l-rikhtechi@phd.araku.ac.ir
Vahid Rafe*
Department of Computer Engineering, Faculty of Engineering, Arak University, Arak 38156-8-8349, Iran
v-rafe@araku.ac.ir
Afshin Rezakhani
Department of Computer Engineering, Faculty of Engineering, Ayatollah Boroujerdi University, Boroujerd, Iran
rezakhani@abru.ac.ir

Received: 15/Jul/2020 Revised: 25/Aug/2020 Accepted: 01/Jan/2021

Abstract
Nowadays, Security Information and Event Management (SIEM) is very important in software. SIEM stores and monitors events in software and unauthorized access to logs can prompt different security threats such as information leakage and violation of confidentiality. In this paper, a novel method is suggested for secured and integrated access control in the SIEM. First, the key points where the SIEM accesses the information within the software is specified and integrated policies for access control are developed in them. Accordingly, the threats entered into the access control module embedded in this system are carefully detected. By applying the proposed method, it is possible to provide the secured and integrated access control module for SIEM as well as the security of the access control module significantly increases in these systems. The method is implemented in the three stages of the requirements analysis for the establishment of a secure SIEM system, secure architectural design, and secure coding. The access control module is designed to create a secured SIEM and the test tool module is designed for evaluating the access control module vulnerabilities. Also, to evaluate the proposed method, the dataset is considered with ten thousand records, and the accuracy is calculated. The outcomes show the accuracy of the proposed method is significantly improved. The results of this paper can be used for designing an integrated and secured access control system in SIEM systems.

Keywords: Software; Logs; Security Information and Event Management; Integrated Access Control.

1- Introduction

The ever-increasing expansion of software as a major element in everyday activities and the high cost of program failure has led to the emergence of tools for evaluating software. The software has been made for many years and its security has been taken into account more or less. Moreover, as threats become smarter, software security has become more and more important. Security is a requirement that should be considered in software [1]. On the other hand, today one of the most important categories is to monitor users' behaviors in access to available resources [2]. The precise choice of access control model and its security on SIEM systems play a key role in the security of these systems [3]. SIEM systems are located alongside the software and monitor all the events happening in them [4, 5]. These systems have access to all of the information in the programs, and in fact, they are a complete repository of all the events that occur in software. Suitable security measures are taken on software [6], but neglecting the security of the SIEM system overwhelms all the security measures of software; this is due to the access of SIEM systems to all events within the software. If the security of these systems is not properly considered, in addition to threatening the event management system, the software and all its information are also threatened. Failure to pay attention to the access control module's threats can cause malicious and irreparable damages to software and SIEM systems [7]. This study proposes an approach not also for creating the SIEM system for software, but also for applying a proper and integrated access control module in these systems based on new standards and access control models [8, 9, 10]. All key points in SIEM that require access to information for generating, storing, analyzing, and monitoring security events are specified and access control is carefully done at all points. All threats to the access control module are identified and solutions are suggested to reduce these threats.

2- Related Works

Here are some recent works on the subject of this paper. Nazir et al. (2016) conducted a study aimed at proposing

high-level language for managing information and security events [11]. In the paper, a Data Specification Language is introduced that simplifies the generation of law for information management systems and security events. Di Sarno et al. (2016) studied the information management systems and security events that solve disparities in security policies [12] and discover the unauthorized network data paths and appropriate configurations for network tools. Granadillo et al. (2016) proposed two new approaches to correlation alert [13]; the previous depends on strategy requirement and safeguard ability models, and the last depends on data security markers. Grambow et al. (2016) [14] provided a background on the existing technical challenges and a practical approach to the Context-mindful Software Engineering Environment Event-driven system (CoSEEEK). This research shows how to use automatic knowledge in creating processes, process compatibility, and environmental process support. In a previous study by the authors of this paper, it was noted that to have a comprehensive AAA model, AAA requirements should be carefully considered through multilayer security policies [15]. For the doctoral dissertation, Grispos (2016) conducted an exploratory case study in an organization to practically address the security events in organizations [16]; therefore, several evaluations of SIEM have been investigated in a case study of an organization. Betz (2016) examined whether information technology by an organization's financial services company can be used to reduce intrusion and security events [17]. B. Mahesh Babu et al. (2015) proposed an advantage the board component that deals with the clients by joining hazard, trust into an entrance control system to build up a more versatile and adaptable avoidance instrument against insider assaults [18]. The paper [26] proposed an autonomous log stockpiling the board convention with a blockchain technique and access control for the IoT climate. The independent model permitted sensors to scramble the logs before sending them to the passage and worker with the goal that the logs were not uncovered to people in general during the correspondence cycle. As per one exemplification, when a SIEM gadget acquired a security occasion, a danger level of the security occasion was determined dependent on at any rate a connection of the security occasion with at least one resource ascribes of an organization that was overseen by the SIEM gadget [27]. The utility of a convenient purchaser gadget was stretched out by permitting account holders the capacity to acquire section into access-controlled scenes utilizing a compact customer gadget that was related with a record that was utilized to buy the affirmation or passes to the occasion at the entrance controlled setting [28]. A summary of the above-discussed related studies is presented in the Table1.

Table 1. Comparison some of the related works

Author/s	**Description**	Advantages	**Disadvantages**
Nazir et al [11]	An undeniable level area explicit language for SIEM (plan, development, and formal check)	Providing a language for managing information and security events	Lack of standard rules to be used in other security systems.
Di Sarno et al [12]	An epic security data and occasion the board framework for improving online protection in a hydroelectric dam	Explaining information management systems and security events where differences in security policies are resolved	Lack of broad test examinations to investigate the adequacy of the SIEM framework in basic foundation applications.
Granadillo et al [13]	Novel Types of Correlation between Alert for Event Management Systems	Proposing correlation between alert approaches. The former is based on models of defense and compulsory policy, and the latter depends on data security markers	PIP and PDP are access control blocks and in this paper, the exact relationship of access control with proposed SIEM is not specified.
Grambow et al [14]	Context-Aware and Process-Centric Knowledge Provisioning: An Example from the Software Development Domain	Providing background on the existing technical challenges and a practical approach to Context-aware Software Engineering Environment Event-driven framework (CoSEEEK)	Lack of software security approach in secure software development
Rezakhani et al [15]	A novel multilayer AAA model for integrated software	Providing a comprehensive approach that defines AAA design for both the operational and executive level and the organizational level	Ignore system logs for more accurate access control
Grispos et al [16]	On the upgrade of information quality in security occurrence reaction examinations	Examining learning security event in organizations	This thesis does not use integrated access control to obtain accurate data.
Betz et al [17]	an investigation of the connection between Security Information innovation improvements and Computer security penetrates and occurrences	Examining whether information technology by an organization's financial services company can be used to reduce intrusion and security events	Low attention to security information and event management in promoting IT security
Hsu et al [26]	An independent log stockpiling the board convention with Blockchain instrument and Access control for the Internet of Things	propose a free log stockpiling the executive's convention with a blockchain technique and access control for the IoT climate	Inability to check log age and log investigation the board Protocol with blockchain mechanism and Access Control for the Internet of Things
Liang [27]	Security information and event management	Figuring a risk level of the security occasion dependent on at any rate a relationship of the security occasion	Lack of integration between SIEM and software and lack of security between them
De Oliveira et al [28]	Occasion access with information field encryption for approval and access control	Strategies permit cardholder verification in a non-installment setting that empowers cardholders to get to an area or a particular occasion.	Encryption is used for confidentiality but it is not used for digital signatures and access control.

3- Proposed Approach

The focus of this research is on creating an integrated and secured access control in security information and event management systems. The proposed module is provided beside the security information and management system along with the software.

The SIEM must have full access to all information and events within the software and analysis event correlation [19]. All access to generated logs must be carefully monitored to prevent information leakage and other security threats. Therefore, integrated access control has a key role in establishing the authority level in the proposed conceptual model [20]. The conceptual model is presented in Figure 1.

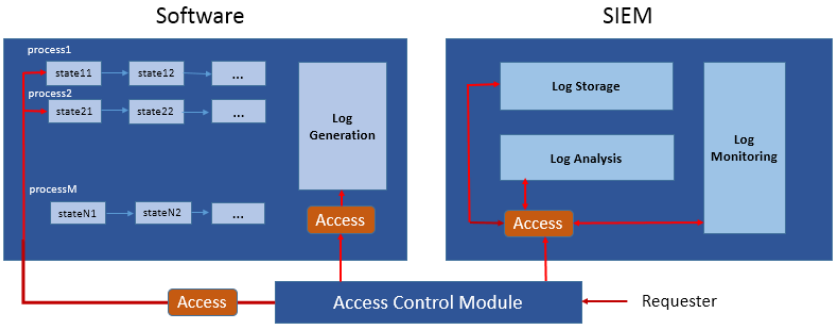


Fig. 1. General Conceptual Model

As shown in the above figure, various components are used to manage the software logs. These components include log generation in the internal structure of software, as well as log storage, log analysis, and log monitor in the SIEM structure. All sections require to store or retrieve logs. Therefore, the access control module is defined as the central point to manage access of all components requesting logs in SIEM. The proposed levels for access management in SIEM is shown in Figure 2.

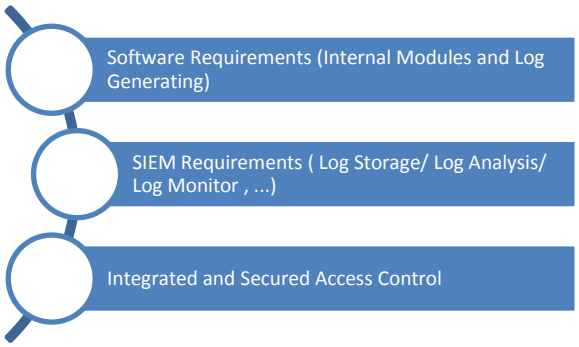


Fig. 2. The proposed levels for access control in SIEM

3-1- Software Requirements

The first step in creating the access control module in SIEM is to make the requirements in software. The software must be created based on software development standards; hence, ISO/IEC 12207 [8, 9, 21]. It is necessary to designing the components for log generation, designing components for securing logs, and also designing the components to logs access. The effective factors in software for creating the SIEM system and access control module are as follows:

I. **Using ISO/IEC 12207:2017 as a deployment guideline:** the ISO/IEC 12207:2017 standard generates software from the perspective of functionality and non-functionality requirements. It even considers the organizational perspective and defines the life cycle for software development. Therefore, this standard is used as a guideline for determining the requirements and the necessary processes and designing a secure architecture for the creation of software.

II. **Designing components for log generation:** After defining the software requirements, the processes to meet the logs generation need to be identified. Accordingly, based on the XES template following the IEEE 1849-2016 standard, the logs' format is determined [22, 23]. The emphasis of this paper is on the generation of those logs that record activities within the business processes. Therefore, logs contain items such as process numbers and activity numbers within processes. After generating the logs, in addition to storing the generated logs in SIEM, they are also stored in software repositories.

III. **Designing components for securing logs:** It is necessary to identify all the general and specific requirements that are needed to secure the logs. One of these requirements is to create and secure log files as well as securing communications to access these files and also syncing logs within the software and SIEMs.

IV. **Designing the components to logs access:** Another requirement to be considered within the software is to

design access control capabilities that will be required during production or use of logs. The reason for designing access control in software is that all events within the software are accessible in the log generation process, and failure to consider the security will result in information leakage. Therefore, it is necessary to create an access control capability for accessing the logs being generated and already generated.

3-2- SIEM Requirements

By doing the above steps in software, the conditions are provided to create the initial requirement in the SIEM system which is capable of storing, analyzing, and monitoring logs. The SIEM system can receive the required logs in the XES format in the IEEE 1849-2016 (IEEE Standard for eXtensible Event Stream (XES) for Achieving correlation of events) [22, 23] and take the appropriate action. The following main components should be considered in designing the SIEM system:

I. **Log Storage:** This block is used to receive logs from the log generation block within the software in the XES format and store them in SIEM.
II. **Log Analysis:** This block is used to analyze the logs stored in SIEM. Determining the correlation between events is one of the most important tasks of this block, which analyzes the logs and extracts the correlations between the events. Event analysis can be used to detect users' suspicious behaviors.
III. **Log Monitoring:** After storing and analyzing events, logs and correlations should be monitored.

The next step for deploying access control module in the SIEM is to provide key points for giving users access permission. In other words, all the key points in which the authority level of users in the SIEM should be investigated are determined. Some of the key points for access control are as follows [24]:

I. **Key points for access control in the log generation block:** Access control in the log generation block is placed on the software side. There are several components in this block, including log generating formatting and log generating parsing. Among these components, the two log-generated storage and log retrieving components are suggested for the users' access control. The access control of SIEM users is performed not only on servers where SIEM is based but also on access to information in software (before sending log information to SIEM) at log generated storing and log retrieving from the log block key points.
II. **Key points for access control in the log storage block:** The log storage block is located on the SIEM system side. This block contains components such as log conversation and log rotation. Among the components of this block, the log storage, log rotation, and log archival key points have access to logs that need to be monitored carefully.
III. **Key points for access control in the log analysis block:** This block is used for event correlation in logs, and contains components such as log retrieving, Rule/policy Definition, Rule/policy editing, Rule/policy deleting, and Reactive Affairs.
IV. **Key points for access control in the log monitoring block:** This block also includes various components in which key access control points include log viewing and alert reporting.

3-3- Integrated and Secured Access Control

The integrated access control module is responsible for issuing access permissions on all software and the SIEM components. The access control module is suggested to use the attribute-based model and architecture described in ISO/IEC 10181. The XACML language is a standard OSSIS language based on the XML and describes security policies. According to this standard, to deal with the requester's request, it is expected to send the solicitation to Policy Enforcement Points (PEP). This unit is given dependents on the reaction to the Policy Decision Point (PDP), as the user interface gives a coherent reaction to the requester. PDP chooses by two fundamental units of Policy Administration Point (PAP) and Policy Information Point (PIP). In PAP every one of the policies is composed by the proprietors and this unit assumes the part of client arrangements knowledgebase. Another unit, Policy Information Point, should exist next to PDP for a dynamic that decides the credits of the requester. PDP gives the authorization of availability dependents on the arrangements in PAP and the requester data in PIP [15]. The access management is to check if the SIEM components are allowed to access the requested information (for storing, retrieving, analyzing, etc.). In an integrated access control module, the applicant within SIEM sends the request for access to the required information to the policy enforcement point. The policy enforcement point inquiries from the policy decision point and decides to issue permission to access or deny access based on the received response.

On the other hand, threat modeling is a way to deal with security examination. This sort of modeling is an organized methodology that empowers planners to recognize, measure, and right the risks. It is suggested to examine the access control module designed for the SIEM system in terms of different threats. The main feature in creating threat modeling will be to reduce potential insider/outsider threats to the integrated access control module. During the explanation of any internal/outsider threat, suggested solutions to decrease them are provided as well.

3-3-1- Insider Threats (Abuses) & Proposed Safeguards

Insider threats (abuses) are the potential threats to the access control module that issue unauthorized access permissions to well-known users. These threats can occur intentionally or unintentionally, but they do have a devastating impact on the accuracy of the access control module. Insider threats (abuses) can have different effects on the SIEM system.

By ISO/IEC 12207:2017 a secure architecture should be created for the access control module in the SIEM system. The proposed architectural design is used to describe the functional requirements as well as non-functionality requirements. The architecture of the secured access control module is presented in Figure 3.

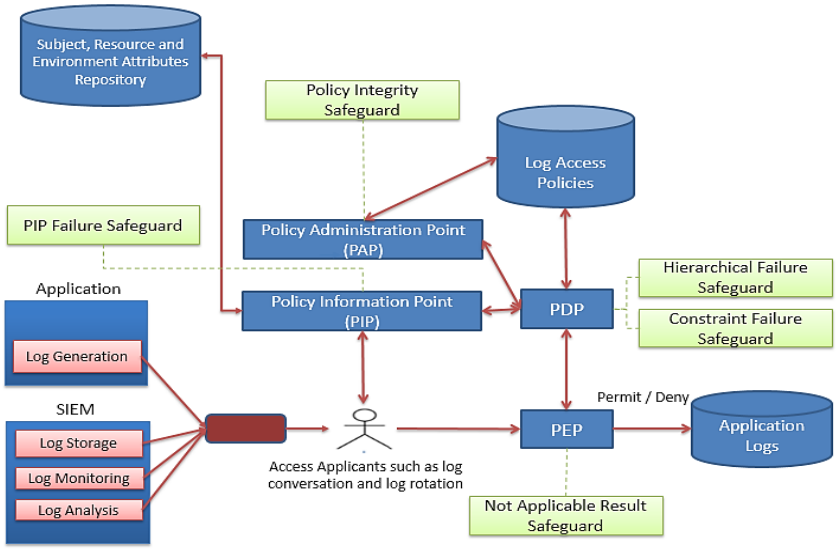


Fig. 3. The Secured architecture of the access control module of SIEM

After examining different insider threats of the access control module, the discovered abuses and proposed safeguards can be accurately categorized as follows:

I. Insider PIP Failure & Safeguards

In process of issuing access permissions, the attributes of the requesting user are compared with the policies in the policyset, and the access permissions are issued to the users at the above listed key points. However, the characteristics of the requester may not be recognized for any reason. In this case, the access control module cannot map the policy to the requestor and therefore the module may make a wrong decision. Among the internal factors that can cause this threat are the tools and technologies used to protect privacy.

The solution to this vulnerability is to use appropriate privacy engineering methods. Given that the proposed access control module is defined in the form of an integrated manner, access control policies and privacy policies are defined accordingly. This will always allow the access control module access to the requesting attributes, and the PIP failure problem will not occur.

II. Policy Integrity Failure & Safeguards

One of the potential threats to the access control module is the lack of a mechanism for policy integrity. Different parts of the organization may use different repositories for access control policies. As a result, policies may interfere by mistake. Internal users just need to exploit this vulnerability in the access control module and create conditions in which their access policies are selected and reviewed by them from their predetermined repository, and therefore, they access unauthorized resources.

In the proposed approach, to fix the problem, policyset, policy, and rule structure are used to define access control policies. The structure of policies is in this way that there are several policysets. Each policyset contains several policies and each policy contains several rules. This kind of definition allows policies to fit into this structure according to different conditions. Applying this structure to define access control policies in a unified and managed way can accommodate all conditions and control accesses.

III. Not Applicable Result & Safeguards

This vulnerability occurs when there is no policy defined in the policy repository for the user's attributes. In this case, the access control module cannot make the right decision. Therefore, it is enough that the internal user attacker provides situations where there will be no policies on his or her attributes, and by most of the access control systems, the access permission will be issued to him.

The suggested solution is to use deny-override and permit-override policies according to the level of trust of users. The deny-override policy means that the access control module will not allow access if no policy is found for the requestor. Also, the permit-override policy means that if the access policy is not found for the requestor, it is granted access. It is recommended that the access control module use the permit-override policy if the requestor trust level is above a certain level and the deny-override policy if the requestor trust level is lower.

IV. Hierarchical Failure & Safeguards

Occasionally due to mistakes made by users in the access control module, restrictions may be occurred and lead to unauthorized permission. Wrong restrictions are an insider threat and abuse can even deny authorized users. For example, the hierarchical failure threat leads to define a series of constraints for an existing user (due to a role inherited from another role) intentionally or unintentionally. In this case, although the user should have access to specific information due to inheritance, the definition of inappropriate constraints will affect his access. The proposed approach to prevent this vulnerability is to develop policies to control roles when defining new constraints. Thus, if inheritance exists between roles, it will not be possible to define any constraint, and only constraints can be defined that do not impair inheritance.

V. Constraint Failure & Safeguards

Different constraints can be defined for access by users of the SIEM system in the access control module. For example, suppose that two roles are inconsistent pair-wisely. This means that these two roles are not attributable to a user. However, the user acquires permissions via a role inconsistent with their current role in any way. In this case, access to the SIEM is unauthorized and causes information leakage. One of the examples leading to unauthorized permission is the inheritance from the roles.

In other words, due to user mistakes in the access control module, the inheritance of the roles may be mistaken and cause an invalid authorization to a role. This off-base inheritance is an insider threat and abuse. For instance, assume an authorized user in the access control module has a user permission definition. Therefore, while defining a new user, the new user inherits an existing role intentionally or unintentionally. In this case, the newly created user will have all of the parent user permissions, and if it is done incorrectly, it can cause information leakage.

To prevent this vulnerability, the definition of new inheritances is controlled over roles. In a way that, if there are constraints between roles, it will not be possible to define inheritances that violate those constraints. In this case, the only inheritances can be defined that do not impair the existing constraints. Because otherwise it may be denied access through the extinct of the constraints, but because of the inherently wrong definition, this allowance is done by error.

3-3-2- Outsider Threats (Misuses) & Proposed Safeguards

Outsider threats (misuse) include those threats that are exerted by outsourced and unauthorized users on the access control module. These types of threats are usually imposed on the system due to vulnerabilities in the access control module. In this section, the outsider threats that enter the access control module of the SIEM system are identified and categorized. These types of threats have a very destructive role in reducing SIEM security.

I. Misuses

Sometimes the failure to identify the characteristics of the requester isn't because of inside reasons however relies upon untouchable causes. One of the elements that can cause untouchable dangers can be DoS attacks on servers that cause their servers to break. The breakage of servers that hold the user characteristics will cause the PDP failure to receive the necessary information to make a proper decision. The XACML language does not have any solution to maintain confidentiality in remote users' communications with the SIEM server. This threat is a misuse and can disrupt SIEM work or disclose information among users. Another type of outsider threat that can be created by individuals outside the organization is the message replay. The attacker person can save the solicitations and replay them at the time of the attacks. In another sort of threat, an outcast attacker sends messages among the legitimate messages that the SIEM clients are sending and causes various problems. In another kind of threat, the attacker modifies messages between SIEM users. This kind of threat is very dangerous because the attacker can change the unauthorized decision into an authorized one. Another kind of outsider threat that can enter the SIEM system is to attack the PDP. In this threat, the attacker tries to send a large number of messages to the PDP. This threat causes a failure in PDP.

II. Safeguards

Some of the problems mentioned above, such as the DoS attacks, are not addressed in this article. However, other problems such as breach of confidentiality, Message replay, Message insertion, and Message modification can be remedied by using software certificates within SIEM and requiring the use of these certificates in communicating SIEM with the access control module. The suggested solution is to use a valid certificate authority to create digital certificates and use them within SIEM. The algorithm of the proposed secured access control module in terms of outsider attacks is as Figure 4.

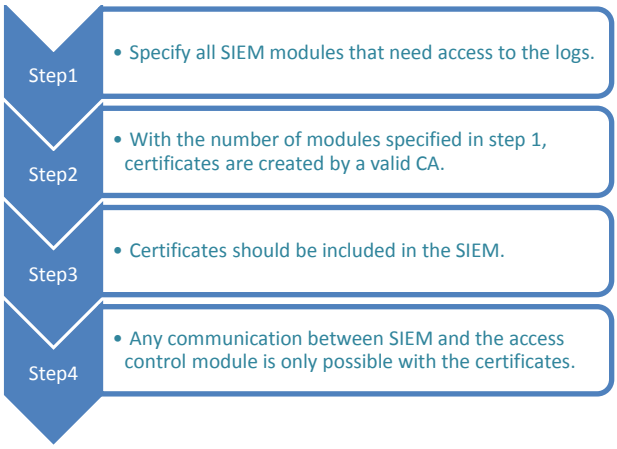


Fig. 4. The algorithm of secured access control in term of outsider attacks

4- Implementation and Evaluation

In this section, the proposed model will be implemented and evaluated. At first, the case study is discussed in detail and the proposed method will be implemented. Then it will be evaluated in terms of insider and outsider threats.

4-1- Implementation

Along with the implementation of the SIEM in this study (including requirements analysis, architectural design, and coding), the specific access control module is designed and produced, which is responsible to control access to receiving and analyzing software events. The SIEM system has various capabilities through which the users defined can access all the events in software and saves, analyzes, and monitors the events. Before implementing the access control module, the implementation conditions must first be specified. In this case, the blocks defined in specific SIEM in the system are presented in Table 2. Also, the number of roles and users applied to use SIEM in the presented software are listed in Table 3.

Table 2. Defining the blocks in SIEM

	SIEM block	Abbreviation
1	Block of Log Generation	LG
2	Block of Log Storage	LS
3	Block of log analysis	LA
4	Block of log monitoring	LM

Table 3. The number of roles and users in SIEM

	Name	Numbers	Example
1	Users	20	User1
2	Roles	9	LA manager, LA user
3	Permissions	21	Read, Write

Table 2 shows the blocks requested by the subjects. For example, log generation blocks are used to create logs in the software. The log storage block is used to store logs and the log analysis block is also used to analyze logs. Table 3 defines the users, roles, and permissions in the implemented access control module. For example, 20 users are defined in the system, and also the roles of the LA manager and LA manager in the access control module are defined.

Step 1: Requirement analysis

By Standard ISO/IEC 12207:2017 (Systems and software engineering – Software life cycle processes), security requirement analysis should be done to deploy an access control module. These requirements are expressed in terms of use cases. In the use case diagram, in addition to the main cases to create the access control module, some issues will reduce the insider threats of the module. The issues raised as the functionality requirements of the access control module in the SIEM system are as follows:

- Policy Enforcement point
- Policy administration point
- Policy Information point
- Policy Administration point

As shown in the previous section, insider threats were suggested during requirement analysis. Now the non-functional requirements of the access control module to reduce the insider threats should be determined as follows:

- PIP Failed safeguard
- Policy administration point Integrity
- Not applicable result safeguard
- Hierarchical Safeguard
- Constraint Safeguard

Step 2: Secured Coding

By performing the above steps, all conditions for the implementation of a secured access control module for the SIEM system are provided. At this point, the access control module is built according to the security requirements expressed in the first step. Insider threats that are entered by the internal authorized users of the access control module into the SIEM system are controlled for the prepared verification checklist.

In addition to the above-mentioned insider threats, the module also controls the outsider threats that come from outside of this module. To reduce outsider threats we are deployed certificates within the SIEM. First, Root CA is installed on the Windows server and we use it as a certificate issuer. Next, the certificates are issued for the components of log generation, log storage, log analysis, and log monitoring. Finally, we embed these certificates into the above components. Therefore, each component associates with the certificate created on a secure platform with the access control module.

4-2- Evaluation

In this section, the proposed method will be evaluated and compared with the recent methods. One of the

problems in evaluating and checking the accuracy of the proposed method is the lack of any standard and dataset in this context. So first, a dataset is created randomly with 10000 records to observing the effective features for evaluation, and then the accuracy parameter will be examined carefully. The created dataset features that we call TMDS are provided in Figure 5.

The TMDS dataset contains several features that play an essential role in granting access. The first features are the requester's name and part of the software from which the access request was issued. Requester location and request time are other fields. The role and level of trust of the requester are other features of the dataset. The business process and the state from which the access is requested are also other features of this dataset. In addition to resource, action, and grant, the hierarchical roles and constraints between roles as well as the policies repository are also the features of the TMDS dataset. We have completely randomized this dataset with 10,000 records. One of the data records shown in Figure 5 means that user1 in the log-storing process, within the organization at 8 am and with the role of LS_LS if the trust level of the user is 0.6, the permission is permitted to write on the log. This is the case if it conflicts with the role of LS_LR and Repository1 is also the repository of policies.

FEATURE NAME	Requester_Name	Requester_Position	Requester_Location	Request_Time	Requester_Role	Requester_Privacy	Process	State	Resource	Action	Grant	Hierarchical_Roles	Constraints_Roles	Policies_Repository
Record0	User1	Log Storing	Enterprise	8:00	LS_LS	0.6	Log Store	Log Storing	Logs	Write	Permit	---	LS_LR	Repository1
	.	.	.	.	.	.	.	.	.	.	.	.	.	.

Fig. 5. The provided dataset features

4-2-1- Insider Threats Reduction

To evaluate the proposed access control module, the accuracy parameter in association with insider threats is validated. Verification and validation checklists have been used to consider some of the insider threats related to the proposed module. This checklist is used to validate the access control module against the PIP failure attack. The verification checklist for this threat is in Table 4.

Table 4. Verification checklist for PIP failure threat

	Verification List	Explanation	Classification
1	ISO/IEC 12207 applies to software production	Application of ISO 12207 standard in software development phases	Discretionary
2	Use privacy engineering policies	Using privacy engineering to respect the privacy	Discretionary
3	Implement ISO 10181 correctly	Use ISO 10181 to grant access permissions	Discretionary
4	Identify access decision-making components	The decision-making components include PDP, PIP, PEP.	Mandatory
5	Communication between software modules is not limited	No restriction on sending information between decision components	Mandatory
6	The PIP module does not restrict the sending of user information to the PDP	Unlimited sending of information from PIP to PDP upon request	Mandatory

We also designed a tool called *Test Tool* to check the accuracy of the access control module against other insider threats. With the designed tool, for each threat, we check the access control module before and after applying the proposed method. In Figures 6 and 7 two parts of this tool are shown to determine the accuracy of the module in Hierarchical Failure and Constraint Failure threats.

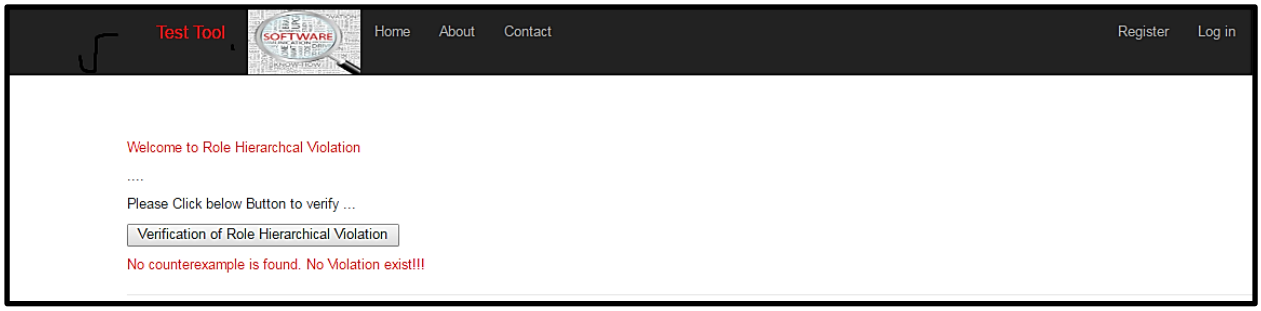


Fig. 6. Role hierarchical verification in the Test tool

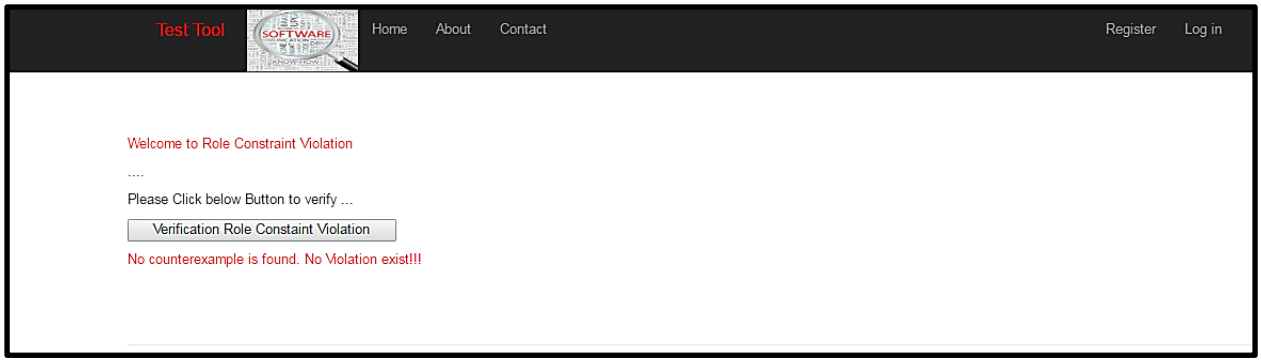


Fig. 7. Role constraint verification in the Test tool

To evaluate the access control module, it is necessary to calculate the confusion matrix parameters. For this purpose, the following values are defined:

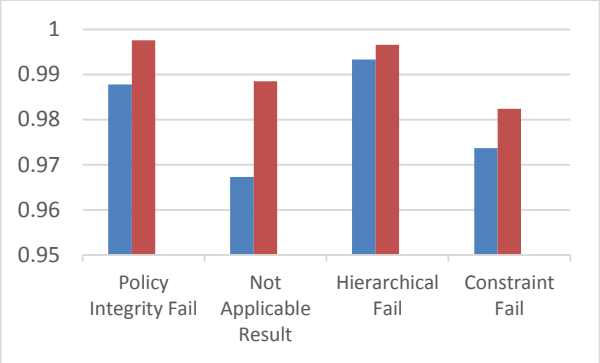
- ✓ TP: The number of records of the TMDS dataset that issue access permissions correctly.
- ✓ TN: The number of records of the TMDS dataset that do not issue access permissions correctly.
- ✓ FP: The number of records of the TMDS dataset that issue access permissions incorrectly.
- ✓ FN: The number of records of the TMDS dataset that do not issue access permissions incorrectly.

According to these values, the parameter of accuracy is calculated in the formula $\text{Accuracy}=\frac{TN+TP}{TN+FN+TP+FP}$. The accuracy parameter is calculated for PIP failed Results, Policy Integrity Failed, Not applicable result, Hierarchical Fail and Constraint Fail threats. According to the information in our TMDS dataset, the TP, TN, FP, and FN parameters are calculated after utilizing a secured access control module for each of the insider threats discussed above, along with the parameters to be evaluated in Table 5.

Table 5. The accuracy calculated for each insider threat

	Policy Integrity Failure	Not Applicable Result	Hierarchical Failure	Constraint Failure
True Positive	5022	5034	5015	4783
True Negative	4954	4966	4951	5041
False Positive	12	116	0	94
False Negative	12	0	34	83
Accuracy	0.9976	0.9885	0.9966	0.9824

As can be seen, accuracy is calculated for each of the insider threats after using the proposed access control module. For each threat, the true positive, true negative, false positive, and false negative are calculated, and then the accuracy is obtained using the defined formula. For example, for the Policy Integrity Failure threat, the accuracy parameter is 0.9976. The accuracy is calculated for the rest of the insider threats as shown in the table above. Also, the accuracy parameter is compared before and after using the proposed method and is shown in Figure 8.



Blue bar: the accuracy before any insider threat reduction
Red bar: the accuracy after any insider threat reduction

Fig. 8. Accuracy before and after of any insider threat reduction

4-2-2- Outsider Threats Reduction

In the previous sections, the access control module is evaluated in terms of insider threats. In this section, the access control module embedded in SIEM is evaluated in terms of outsider threats. The acunetix tool is one of the tools for analyzing and detecting software vulnerabilities [25]. This tool provides alerts based on malicious targets' access paths at four levels:

1. *High:* The highest level of vulnerability, which is very dangerous and allows the hacker to control the software;
2. *Medium:* The medium vulnerability level is less than the previous one, but there is still the ability to control the software;
3. *Low:* It has the lowest risk and ordinary hackers cannot access the software;
4. *Information:* A warning to prevent theft of information

At first, by using the acunetix tool, the vulnerabilities in the access control module are examined. At this step, no action has been taken to utilize the certificates. Then, based on the description of the previous section, the SIEM components communicate via software-defined certificates with the proposed access control module. Finally, the vulnerabilities in the access control module are re-examined by the acunetix tool. The results of the evaluation of threats are provided in Table 6.

Table 6. The number of security alerts for outsider threats

	Informational Risk	Low Risk	Medium Risk	High Risk
Before Proposed Method	5	4	2	5
After Proposed Method	1	1	1	2

5- Conclusion

In this paper, a new method was developed to enhance the security of the access control module in the SIEM system. First, all key points that are accessed by the SIEM within the software are identified and then policies are developed to control precise access. Also, the threats entered into the access control module are carefully detected and then decreased. To assess the proposed method from the perspective of insider threats, the parameter of accuracy was calculated. Also, the number of vulnerabilities was calculated to evaluate the proposed method based on outsider threats. By applying the method proposed in this study, it is possible to enhance the security of the access control module in SIEM systems.

References

[1] D. Godoy and A. Corbellini, "Folksonomy-Based Recommender Systems: A State-of-the-Art Review," Int. J. Intell. Syst., vol. 31, no. 4, pp. 314-346, 2016.
[2] Mohammed, N. M., Niazi, M., Alshayeb, M., & Mahmood, S. (2017). Exploring software security approaches in software development lifecycle: A systematic mapping study. Computer Standards & Interfaces, 50, 107-115.
[3] DURAIRAJ, S. K. J., & Singla, A. (2017). U.S. Patent Software No. 15/303,771.
[4] Detken, K. O., Jahnke, M., Kleiner, C., & Rohde, M. (2017, September). Combining Network Access Control (NAC) and SIEM functionality based on open source. In Proceedings of the 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Software (IDAACS), Bucharest, September 20th till September 23rd.
[5] Miller, D. R., Harris, S., Harper, A., VanDyke, S., & Blask, C. (2010). Security Information and Event Management (SIEM) Implementation (Network Pro Library). McGraw Hill.
[6] Layton, T. P. (2016). Information Security: Design, implementation, measurement, and compliance. Auerbach Publications.
[7] Piessens, F., & Verbauwhede, I. (2016, March). Software security: Vulnerabilities and countermeasures for two attacker models. In Proceedings of the 2016 Conference on Design, Automation & Test in Europe (pp. 990-999). EDA Consortium.
[8] Shostack, A. (2014). Threat modeling: Designing for security. John Wiley & Sons.
[9] Aydan, U., Yilmaz, M., Clarke, P. M., & O'Connor, R. V. (2017). Teaching ISO/IEC 12207 software lifecycle processes: a serious game approach. Computer Standards & Interfaces, 54, 129-138.
[10] López-Lira Hinojo, F. J. (2014). Agile, CMMI®, RUP®, ISO/ IEC 12207...: is there a method in this madness? ACM SIGSOFT Software Engineering Notes, 39(2), 1-5.
[11] Hu, V. C., Kuhn, D. R., & Ferraiolo, D. F. (2015). Attribute-based access control. Computer, 48(2), 85-88.
[12] Nazir, A., Alam, M., Malik, S. U., Akhunzada, A., Cheema, M. N., Khan, M. K., ... & Khan, A (October 2016). A high-level

domain- specific language for SIEM (design, development, and formal verification). Cluster Computing, 1-15.
[13] Di Sarno, C., Garofalo, A., Matteucci, I., & Vallini, M. (2016). A novel security information and event management system for enhancing cybersecurity in a hydroelectric dam. International Journal of Critical Infrastructure Protection, 13, 39-51.
[14] Granadillo, G. G., El-Barbori, M., & Debar, H. (2016, November). New Types of Alert Correlation for Security Information and Event Management Systems. In New Technologies, Mobility and Security (NTMS), 2016 8th IFIP International Conference on (pp. 1-7). IEEE.
[15] Grambow, G., Oberhauser, R., & Reichert, M. (2016). Context-Aware and Process- Centric Knowledge Provisioning: An Example from the Software Development Domain. Innovations in Knowledge Management (pp. 179-209). Springer Berlin Heidelberg.
[16] Rezakhani, A., Shirazi, H., & Modiri, N. (2018). A novel multilayer AAA model for integrated software. Neural Computing and Software, 29(10), 887-901.
[17] Grispos, G. (2016). On the enhancement of data quality in security incident response investigations (Doctoral dissertation, University of Glasgow).
[18] Betz, L. (2016). An Analysis of the Relationship between Security Information Technology Enhancements and Computer Security Breaches and Incidents. (Doctoral dissertation, Nova Southeastern University).
[19] Babu, B. M., & Bhanu, M. S. (2015). Prevention of insider attacks by integrating behavior analysis with risk-based access control model to protect the cloud. Procedia Computer Science, 54, 157-166.
[20] Bhatt, S., Manadhata, P. K., & Zomlot, L. (2014). The operational role of security information and event management systems. IEEE Security & Privacy, (5), 35-41.
[21] Boucher, P., Wright, M., Cranny, T., Nault, G., & Smith, M. (2015). U.S. Patent No. 9, 197, 668. Washington, DC: U.S. Patent and Trademark Office.
[22] ISO, I. IEC 12207: 2017 Systems and software Engineering-Software life cycle processes., (2017). International Organization for Standardization.
[23] Verbeek, H. M. W., Buijs, J. C., Van Dongen, B. F., & Van Der Aalst, W. M. (2010, June). Xes, xesame, and prom 6. In Forum at the Conference on Advanced Information Systems Engineering (CAiSE) (pp. 60-75). Springer, Berlin, Heidelberg.
[24] IEEE Standard for eXtensible Event Stream (XES) for Achieving Interoperability in Event Logs and Event Streams, (2016), IEEE Std, pp. 1849-2016.
[25] Kent, K., & Souppaya, M. (2006). Guide to computer security log management: recommendations of the National Institute of Standards and Technology. US Department of Commerce, Technology Administration, National Institute of Standards and Technology.
[26] Erturk, E., & Rajan, A. (2017). Web Vulnerability Scanners: A Case Study. arXiv preprint arXiv:1706.08017.
[27] Hsu, C. L., Chen, W. X., & Le, T. V. (2020). An Autonomous Log Storage Management Protocol with Blockchain Mechanism and Access Control for the Internet of Things. Sensors, 20(22), 6471.
[28] Liang, D. (2020). U.S. Patent No. 10,616,258. Washington, DC: U.S. Patent and Trademark Office.
[29] De Oliveira, M. G., & Jatoba, P. (2020). U.S. Patent No. 10,579,995. Washington, DC: U.S. Patent and Trademark Office.

Leila Rikhtechi received the B.S. degree in Computer Engineering from Azad University, arak Branch, Iran in 1999, and M.S. degree in Software Systems from Azad University, south Tehran Branch, Iran, in 2002. Currently she is Ph.D. Candidate in Arak University, Iran. Her research interests include software security.

Vahid Rafe is an associate professor at Arak University. His research interests are model checking, software testing and search based software engineering.

Afshin Rezakhani received the Ph.D. degree in computer engineering from Malek-Ashtar University of Technology, Tehran, Iran, in 2016. Now, he works as assistant professor in the Ayatollah Boroujerdi University, Boroujerd, Iran. His area research interests include Software Engineering, Information Security Management System (ISMS), IT Governance and Management (Cobit and ITIL), and software security.