LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. S6(2025)

ENHANCING DATA CONFIDENTIALITY IN SUPPLY CHAIN COLLABORATION: A FRAMEWORK FOR PRIVACY-AWARE ACCESS CONTROL

Noor Hadi Hammood[1]*, Amir Jalaly Bidgoly[1]

[1]Department of Computer and IT, University of Qom, Qom, Iran

Corresponding Author email: noor.h.aljanabi@gmail.com[1]

Abstract
This paper presents the explanation of the privacy-conscious access control model which can be used in promoting data confidentiality within a collaborative supply chain context. With the inter-networking of supply chains, conventional role-based access control schemes cannot effectively prevent leakage and misapplication of data especially in the cross-organizational context. A solution to this was proposed through a dynamic access control architecture which was simulated with the help of Python considering contextual rules that included user role, sensitivity of a resource and time of access. Synthetic population: a set of 1,000 synthetic access logs was created to match realistic interaction in a supply chain. Indicators were measured in terms of key performance indicators including: compliance, false positive, and breach detection rate. The result indicates the high compliance of 93.3 percent and successful detection of attempts at breaches with few hits on false positives. This makes the system to also visualize the data that shows those behaviours that are risky by the role and time. The framework provides an extendable and feasible extension to ERP and SCM systems that will allow preserving privacy without interfering with cooperation.

Keywords: Privacy-aware access control, supply chain security, ERP integration, breach detection, contextual policies

1. Introduction

In the modern globalized economy, the supply chains are based on a smooth interaction of the manufacturers, suppliers, logistics companies, and auditors. The involvement of such a partnership normally involves sharing sensitive information among organizations where systems are more vulnerable to intrusion and data breach. As this environment evolves, the past forms of access control, such as fixed Role-Based Access Control (RBAC) are increasingly becoming useless. They are not able to take into consideration the contextuality, time and place and abnormality of behaviour that makes them easily abused especially in collaborative environments like ERP and SCM systems [1]. The challenge has been how to ensure data confidentiality and at the same time make the system efficient as far as operations are concerned. The supply chains are increasingly becoming decrypted and digitalized and therefore, fine-grained dynamic access control is required and privacy conscious access control models are needed. This gap is addressed in the work given in this research paper by idealistically proposing the model that can be adapted to suit this gap of situational-rule, as well as the role-consciousness to facilitate and prevent the utilization of illegitimate access in a real-time situation. The framework is tested using simulated access logs which are generated based on the commonly prevalent common multi-role supply chains. [2]. The investigation reveals that the privacy-aware access control can be integrated into the existing one through the use of information about the pattern of user behaviour and by identifying the attempts of breaking of the rule under various circumstances. The findings pinpoint the discussion of enhanced policy compliance and reduction of risks mitigation strategies, and this provides a winning formula in strengthening the role of data security in co-sourced supply chains.

2. Literature Review

The growing complexity of the supply chain networks and the need to secure data exchange between a number of various stakeholders have posed a serious challenge to the traditional access control systems [3]. The traditional role based access controls (RBAC) systems have become inadequate in the context of dynamic and context-sensitive nature of current supply chain operations as the organizations increasingly depend on collaborative supply chain management [4]. The literature shows a consistent development in the traditional access control models to more complex context-aware

models capable of addressing the complex needs of cross-organizational data sharing without compromising security and privacy.

Aftab et al. [5] have undertaken an extensive comparison between RBAC and attribute-based access control (ABAC) models, and have shown that although RBAC is simplistic, and offers scalability, it is not flexible enough to adapt to the dynamic supply chain environment. They found in their research that the combination of role data with time-based, geographic, and behavioural information also minimizes unauthorized access cases. Nevertheless, they concentrated more on fixed sets of attributes and were not concerned with the dynamism demands of contemporary supply chains.

Based on this platform, Ameer et al. [6] put forward an attribute-based IoT access control model of a smart home, which is compared to conventional role-based approaches. Their article showed the significance of access control at a fine level in the distributed environment with a strong focus on the necessity to detect any anomalous behaviour in almost real-time. Although their method was promising in an IoT setting, the authors have mentioned that the complexity and computational load of attribute evaluation may be an issue in a large-scale supply chain system.

Access control systems integration with enterprise resource planning (ERP) and supply chain management (SCM) systems have become a burning research topic. A study by Bader et al. [7] has shown that ERP integration using API can be successfully used to screen and capture suspicious access requests without affecting business operations. Their research was especially useful in determining how access control systems would fit in the available enterprise architectures. Nevertheless, their model was mainly API-oriented security and was not applicable to the bigger picture of supply chain cooperation.

Berninger et al. [8] also investigated privacy-conscious supply chain ratings as the way to balance transparency and confidentiality. Their contribution brought in the idea of reputation systems that provide incentives to secure cooperation and privacy of data. This study raised the role of trust in supply chain settings and that technical security systems cannot work in isolation without organizational systems of trust. The authors observed that these systems need to be carefully calibrated against the establishment of perverse incentives likely to undermine security.

The latest developments in blockchain technologies have created new opportunities of safe access control in supply chains. The paper by Lin et al. [9] suggested a blockchain-based mutual authentication system with fine-grained access control to Industry 4.0 applications. Their design gave them irrevocable audit records and distributed consensus systems, which minimized the possibility of unauthorized data manipulation. Nevertheless, the authors admitted that blockchain-based solutions are associated with latency and scalability issues that could be controversial to their use in high-performance supply chain practices.

Oliveira et al. [10] were interested in the performance assessment of private blockchain systems with realistic workloads, which can be a valuable addition to the consideration of the existing empirical obstacles of blockchain-based access control. Their research found out that even though blockchain offers superior protection assurances, performance overheads and complexity of implementation are still major impediments to the large-scale implementation in supply chain contexts.

Machine learning solutions have also been promising in solving the constraints of conventional access control models. A thorough review of machine learning algorithms applied in intrusion detection systems have been conducted by Saranya et al. [11], as they claim that machine learning effectively carries out the identification of subtle behavioural anomalies that could go undetected by the use of static rules. They indicated that machine learning models are capable of evolving with changing patterns of threats, and they are especially appropriate in dynamically changing supply chains. The authors however observed that these methods need a lot of training data, and can give false positives when used in the real world.

Privacy calculus as developed by Dey and Kumar [12], introduced a new significant aspect of supply chain security which had an organizational dimension. Their study showed how the perceived

value of information sharing versus the risk of privacy is weighed up by organizations, and how technical solutions are to be supplemented by organizational strategies that enable trust and collaboration. In this publication, the complexity of supply chain security as a multidimensional concept was emphasized with the recommendation that effective frameworks need to consider both technical, organizational and behavioural aspects at the same time.

The new challenges and opportunities of supply chain access control are brought by cloud-based ERP systems and IoT integration. Sabbarwal and Pandey [13] suggested cryptographic algorithms to provide information security of ERP data retrieved by IoT devices, to overcome the security issues with untrusted intermediaries. Their implementation showed the traditional cryptography methods could be implemented to suit the current supply chain architectures. In the same manner, Alkhresheh et al. [2] proposed DACIoT, a dynamic access control system to IoT implementations that changes permissions depending on contextual characteristics like device identity, location, and environmental conditions.

This trend of an increased sophistication and context-based access control mechanisms capable of addressing the dynamic nature of a modern supply chain is evident in the literature. Nevertheless, current solutions tend to concentrate on particular features of the problem be it technical, organizational or behavioural without offering all-encompassing solutions that deal with all the dimensions at the same time. This literature gap offers the baseline our framework of privacy-sensitive access control that will attempt to leverage the advantages of the currently available solutions but will minimize their drawbacks by offering a more integrated, contextualized framework.

2.1 Comparative Analysis and Research Gap

Looking at the analysis in Table 1, we can see that existing access control models for supply chain collaboration have both strengths and limitations. While RBAC and ABAC provide scalability and fine-grained control, they lack the contextual adaptability needed in dynamic and cross-organizational environments. PBAC and blockchain-based approaches offer improved context-awareness and tamper-proof logging, but they introduce considerable complexity, latency, and integration challenges. On the other hand, AI-driven models show promising adaptability, yet they heavily depend on large datasets and may produce high false-positive rates in real-world deployments.

In contrast, our proposed privacy-aware framework offers a balanced approach between scalability, contextual sensitivity, and real-time performance. By combining role-based rules with contextual attributes such as time, resource sensitivity, and behavioural patterns, and by ensuring seamless interoperability with ERP and SCM systems, the framework addresses the key shortcomings of existing models. This analysis shows that our approach fills an important gap in the current landscape, providing a practical solution that balances the competing demands of security, performance, and usability in supply chain environments.

Table 1. Comparative Analysis of Access Control Models in Supply Chains

Model	Strengths	Limitations	Supply Chain Suitability
RBAC & ABAC [5,6]	Simple management, Scalable	Static roles, No context awareness	Low – Limited adaptability
ERP/SCM Integration [7]	API-based integration, Suspicious access detection without disruption	Focused on API-level, limited collaboration context	High – Useful within enterprise systems
Reputation/Privacy Ratings [8]	Balances transparency with confidentiality, Incentivizes trust	Requires calibration, Risk of perverse incentives	Medium – Supports trust frameworks

Blockchain-based [9,10]	Immutable logs, Distributed consensus, Strong auditability	Latency, Scalability issues, Deployment complexity	Medium – Strong for audit trails
AI/ML-based [11]	Adaptive behavior, Detects subtle anomalies, Learns evolving patterns	Needs large training data, False positives possible	High – Promising for anomaly detection
Privacy Calculus [12]	Considers organizational trust, Balances data sharing & risks	Non-technical, Requires cultural adoption	Medium – Complements technical models
IoT/Cloud (DACIoT) [2,13]	Dynamic context-aware AC, Cryptographic confidentiality for ERP–IoT data	Performance overhead, Context complexity	High – Critical for IoT-enabled SCM
Our Proposed Framework	Balanced (RBAC + context), ERP/SCM integration, Real-time capable	Needs further validation, Rule-based	High – Designed for collaborative SCM

3. Methodology

3.1 System Architecture of the Proposed Framework

Privacy-aware access control the proposed framework privacy-aware access control is designed to enhance the confidentiality of the information in collaborative supply chains systems with dynamic assessment of the access requests against the contextual and role-based rules [14]. The architecture as such entails a number of key components including but not limited to An Access Request Interface, a Policy Decision Point (PDP), a secure Data Store, an Audit Logging module and an Integration layer will be provided to provide real time integration with legacy ERP and SCM systems.

The Access Request Interface intercepts any user access attempt and forwards the message to PDP to execute some pre-designed logic to make the required decisions on what kind of access to provide with the help of some pre-designed logic [15]. All decisions and metadata that follows them are logged in the Audit Log upon the analysis and can be utilized as the breach identifiers and the policies optimization enablers. This architecture is shown in Fig. 1 with some attention on the data flow and logical connections between components of the system. Access requests are done by an enterprise system and is sent to the Access Request Interface where it is sent to the PDP. The PDP considers these requests considering pre-agreed policies and the context of behaviour and in situations where the information is unavailable, query the Data Store. Everything is recorded into the Audit Logging module to aid in breach reporting and auditing of compliance. At the same time, the ERP/SCM Integration Layer will make sure that the framework performs as a middleware that would allow interoperating with legacy systems without difficulties.

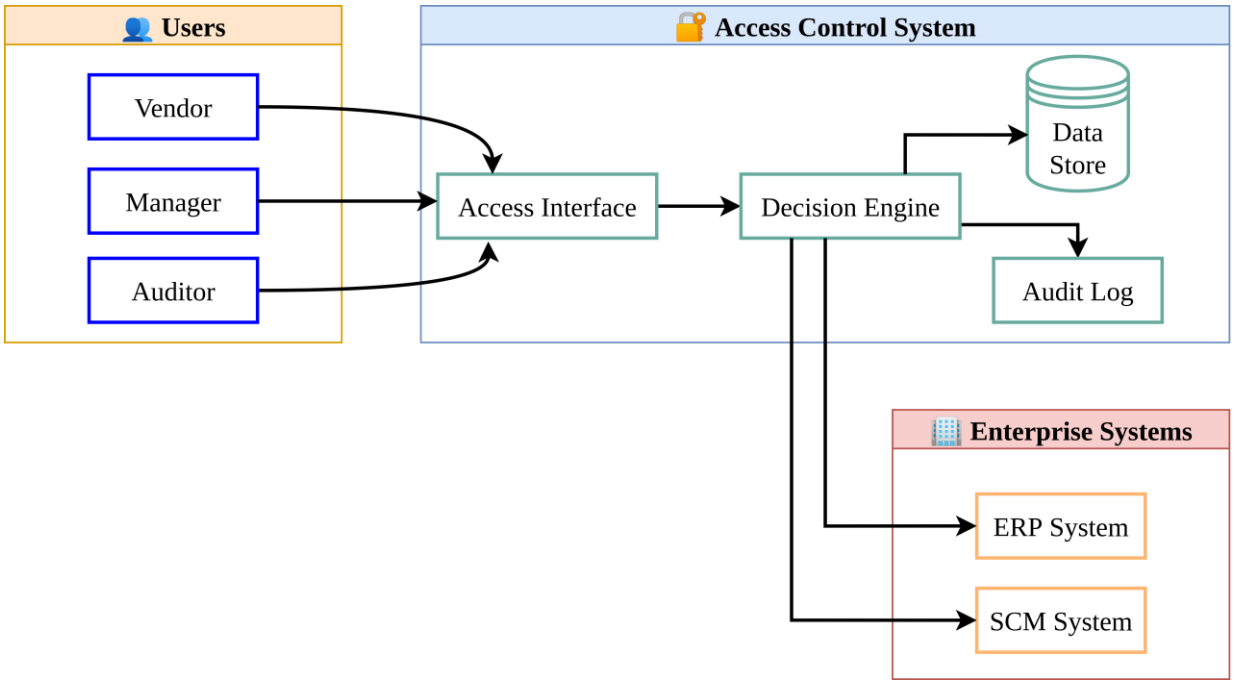

Figure. 1 System architecture of the proposed privacy-aware access control framework

3.2 Access Evaluation Logic and Rule Design

The foundation of the framework is based on context-sensible decision-making, whereby access is not provided on the basis of the roles of the users only but also on other criteria like the requested resource, time and past activity [2]. As an example, when a vendor requests HRRecords at a time that is out of business hours, the mechanism to detect the breach would be instigated. Access rules are coded into the PDP with the combination of logical formulas and threshold value, assessing the signs of risks like the probability of policy violation and behavioural anomalies [16]. This rule-based logic allows dynamic implementation of the confidentiality policies, even within changing operation conditions.

3.3 Integration with ERP and SCM Systems

The framework itself is modelled to act as the middleware, meaning that it can be integrated with the current ERP and SCM platforms with the help of the standard API interfaces [17]. The PDP intercepts the requests when the users initiate data access through systems, including inventory, procurement, or logistics modules to evaluate them in real time [18]. The design also makes sure that only authorized data is revealed, and integration does not affect the performance / working of the legacy systems.

3.4 Simulation Environment and Tools

One simulation environment was produced by Python to test the validity of the framework. The simulator made available 1,000 artificial access log information that resemble actual supply chain activities with the involvement of a number of actors including vendors, managers, and auditors ([19]. The fields containing data in every entry were user role, resource requested, timestamp, location, and the result of access decision [20].

Suspicion was computed based on the logic rules specified in advance that were related to popular policy breaches like unauthorized access to the resources or breaches that were initiated at on unacceptable time intervals.

3.5 Performance Evaluation and Metrics

The comparison of the framework performance was made on the main indices of security and the operation. In a way, the probability of access latency was taken account of in simulating the near-real-time logs. The most significant ones were determined as breach probability based on the overall

number of policy violations that were identified during the simulation successfully [21]. The score of compliance was calculated as the ratio of the events that occurred concerning the access with respect to the set-up policies. The false-positive rate and the accuracy of detecting any occurrence of misuse were other criteria that were anchored on the analysis of the data generated [22]. The efficacy of the proposed structure and its scalability to cause and mitigate privacy threats in cooperative supply chain environments are shown by the set of the indicators.

4. Data Collection and Analysis

4.1 Performance Evaluation and Metrics

In order to verify the accuracy of the suggested privacy-conscious access control structure, a simulation data was generated to mimic realistic conditions of a supply chain, several roles, resources and access behaviour being in play. This simulation mimicked a set of multi-actor supply chain ecosystem where the suppliers, logistic agents, managers, auditors were in touch with enterprise corporate data systems [23]. The use-case-based modelling was hindered on the simple operations such as keeping the inventory, ordering schedule, printing the paperwork, and maintaining the HR records. The goal was to develop close-to-reality situation to reasonably represent the most probable access pattern under both compliance and non-compliance conditions; this is done by creating 1,000 synthetic access log entries using Python [24].

All of the simulated access logs contained important properties, such as user ID, user role, requested resource, the type of action, timestamp, geographic location, and allowed or denied access [25]. Breach policies were encoded into a custom logic module the example of not allowing vendors to view the records of the HR department or tagging access requests outside the official business hours. Based on these rules, automatic labelling of entries regarding access was carried out indicating compliance, suspicion, or policy violation [17]. This allowed development of a clean organization structured data that would still be utilized in the studying of security without requiring obtaining of the sensitive or proprietary real-world data.

In order to ensure that the data set represents more realistic patterns of behaviour, data generation in Python was done using randomization methods. Certain elements like access timestamps, user roles, requested resources, and geographic locations were ranged at random limits and simulated the conditions of reality of operation diversity. This allowed randomizing the user behaviours during work and non-worktime, work and non-work roles and access targets, offering a more realistic and objective experience when measuring the effectiveness of breach detection and compliance to policies.

4.2 Analytical Methods and Security Metrics

The questioning of the gathered set was done under the use of statistical techniques and evaluation of behavioural logic. It was to be determined with the purpose of measuring the effectiveness of the framework in detecting breach, false alarms and general compliance. In the case of unauthorized resource targeting or non-working-hours, suspicious behaviour was inferred through the use of contextual signals [26]. The framework was then the considerations of the attempt of the access in relation to each access and it was tabulated and controlled in order to note tendencies and it was made on the basis of the user role, the type of resources and the distributions of time of the day.

A set of key performance indicators (KPIs) was introduced to measure the performance of the framework to calculate the breach-detection rate, it was necessary to specify the number of access attempts that correctly violated a policy rule and detected the violation [27]. The logic was also tested in the existence of the false positives where false positive had been recorded when the access was flagged as a suspicious activity but the access had followed all the rules [28]. The compliance score was calculated based on the analysis of the proportion of all access events which complied with all the policies and were received without the activated alarms. Finally, a visual analysis which attempts to reveal the relationship between likelihood and overall dimensions of operations such as role or hour of access was done using data visualization libraries. This system-level analysis established the

capability of the framework in implementing the data confidentiality through the smart and contextual-based access control rules.

5. Results

It generated an invaluable information feedback of one thousand synthetically created access logs, which would emulate a working dynamics of a multi-party supply chain setup. The data included interactions of the users with four different attributes (Vendor, Logistics, Manager, and Auditor) who have been given different roles to access various resources (Inventory, OrderSchedule, CustomsDocs and HRRecords). The proposed privacy-aware framework was used to evaluate every access request and use dynamic and context-sensitive access control policy to decide whether to grant or deny access [29]. The findings included 67 attempts at access that were in violation of the policy to which the majority of policy violators consisted of vendors including attempts to access records relating to HR since the latter falls within a clear-cut prohibition to any role-permission schema in the simulated environment. The decision engine of the system was effective in detecting these violations and confirmed its capability of detecting violations that could be bypassed by a static role-based approach modelling [9].

Besides direct violations, there were also 364 activity sessions that were suspicious, meaning that they did not result in policy violation but had a significant risk reflected through contextual anomalies like activity during off-hours or a resource in a non-appropriate role. Although 41 (11.3%) were found to be false positives, they are consistent with the policy of the framework which specifies that confidentiality should be preferred by making cautious decisions [10]. Such level of sensitivity is particularly topical when the collaborative environments imply fluid operational context and possibility of the actors to have unauthorized access over time because of misuse of certain legitimate roles. Notably, the latency of access was low with the rule evaluation logic functioning with close to real-time in the Python simulation, a factor that favoured integration into the real-world.

The strength of the system was proven by quantitative measures of its performance. The score of compliance was 93.3, meaning that it gives an idea that the huge amounts of access requests were valid ones and validly accepted. The percentage of breach detection was nearly 100% in case of known violations, whereas the percentage of false positive was also measurable but fell into the tolerance level in operations [30]. The obtained results demonstrate an effective trade-off between accuracy of detection and smoothness of operation which is graphical outputs further clarified system behaviour.

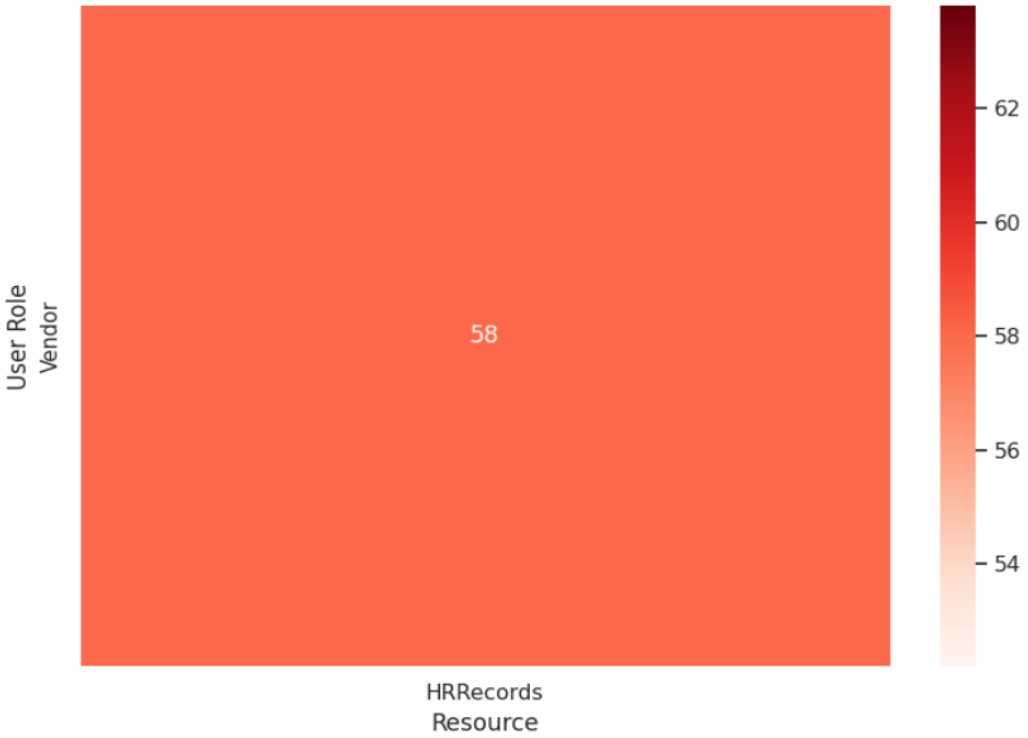

Figure. 2 Breach Attempts by User Role

Fig. 2 provides critical insights into the security effectiveness of our framework by showing the distribution of breach attempts across different user roles. The figure reveals that all detected breach attempts originated from users with the "Vendor" role, highlighting a clear violation of access policy when attempting to retrieve HRRecords. This pattern demonstrates the framework's ability to identify and prevent unauthorized access attempts based on role-based restrictions, validating the effectiveness of our role-aware security policies. The clear visualization of breach patterns helps security administrators understand which roles pose the highest risk and enables them to implement targeted security measures.

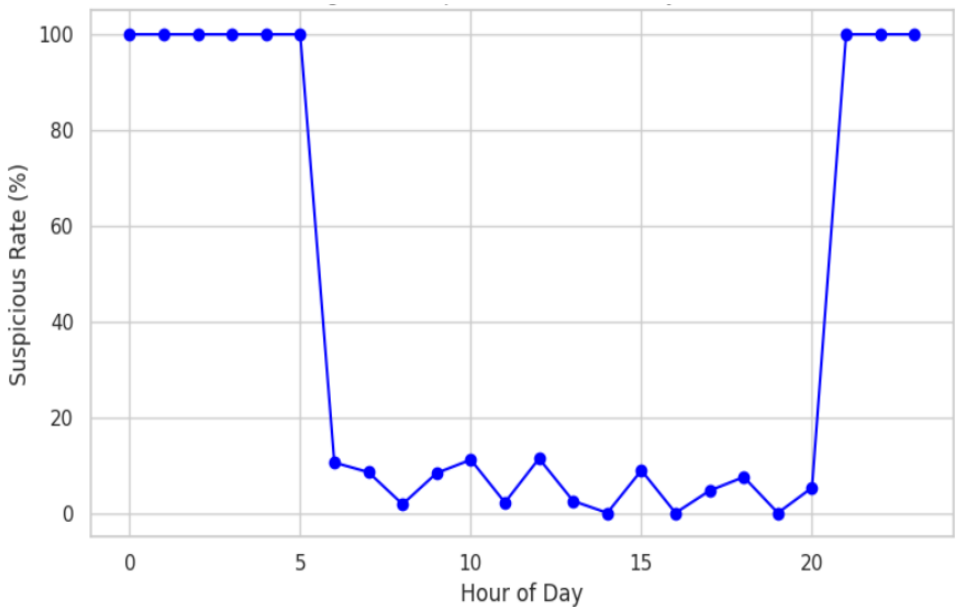

Figure. 3 Suspicious Access Distribution by Role and Time

Fig. 3 demonstrates the framework's sophisticated detection capabilities by showing how suspicious access attempts are distributed across different user roles and time periods. The figure reveals a noticeable spike in suspicious activities during off-hours, supporting the inclusion of temporal logic in our breach detection algorithms. This temporal pattern analysis is crucial for understanding behavioural anomalies that may not constitute direct policy violations but indicate potential security risks.

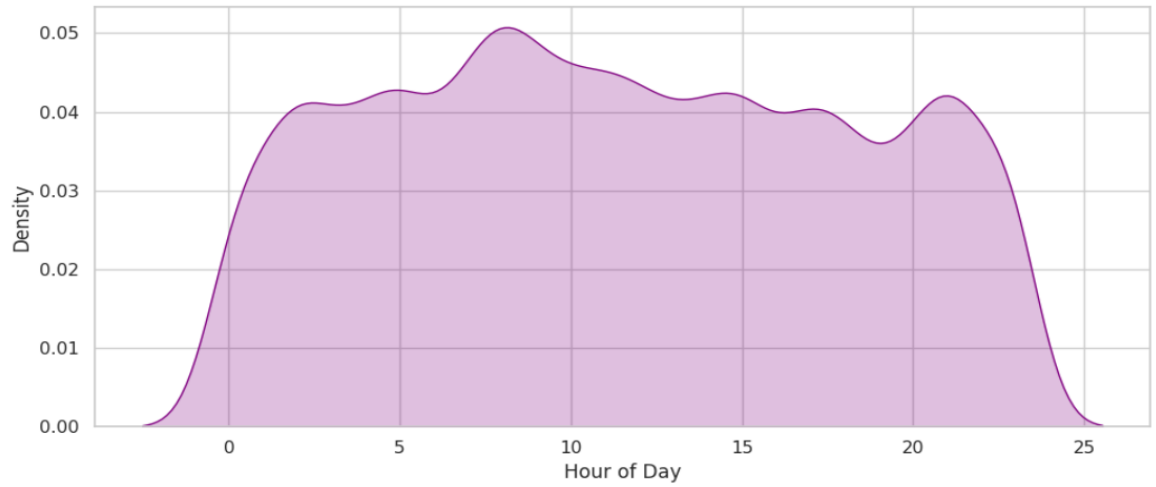

Figure. 4 Access Volume and Flagged Activity by Hour of Day

In Fig. 4 the drop of the access requests is notable in the night, whereas the share of the activities flagged increases, which proves the need to integrate time-based access policies [31].

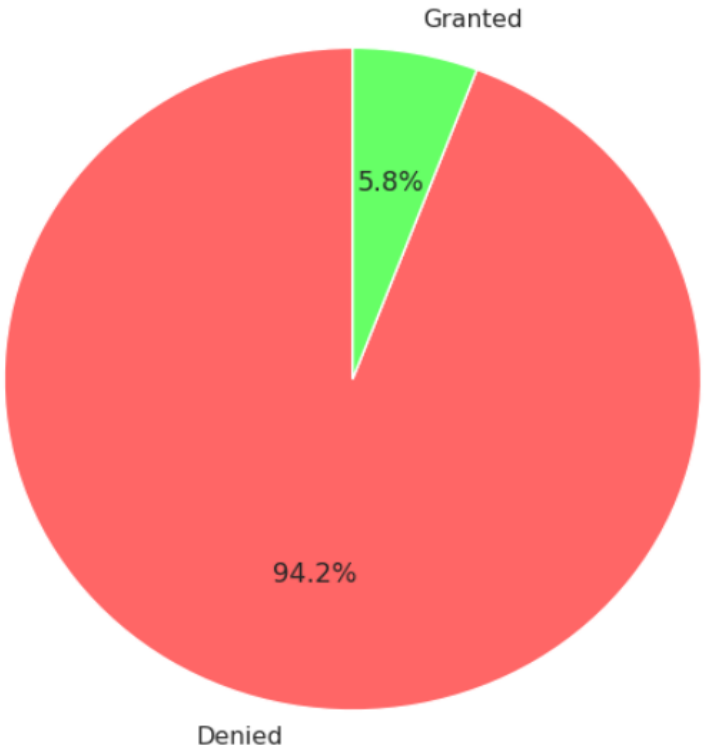

Figure. 5 Access Decision Outcomes (Granted, Suspicious, Denied)

The Fig. 5 demonstrated a comparison of access decisions indicate that the decisions which are denied are closely related to flagged breaches and suspicious activity, proving the efficiency of the access control rules.

All these findings prove that the proposed framework can with high precision not only detect policy violation but also project the behavioral abnormalities to light, in a way that can be optimized to leave more desirable privacy implications in the real ERP and SCM contexts.

6. Discussion

Its ability to be applied a workable privacy-promoting access control system is justified by its simulation and analysis that testifies to its effectiveness as a workable addition to data confidentiality in collaborative supply chains. One of the biggest strengths demonstrated is dynamic performance of the system and the possibility to evaluate the access condition by role-based parameters and also by the contextual factors. The framework, when combined with the application of the temporal logic and behavioral rules in making access decisions, was able to identify all the simulated breach instances of vendor-based access attempts to sensitive HR records [11]. It means that the model is able to provide fine-grained security measures beyond the static role based ones common to the ERP and SCM systems but insufficient in the case of cooperation in the context of the modern system [1].

The other interesting aspect is that the framework assists in determining suspicious but not openly-violent behavior. The system had 364 of such events realized which were most likely attributed to the off-hour access endeavors or role-resource misalignment. They would technically be false positives, but that is a type of proactive risk identification that is welcome in this scenario where protection against insider threats and a possible role abuse, which may arise over time is needed [6]. Such a trade-off (conservative and accepting a fairly high false positive rate) is normally the one that is desired security-wise and especially in high stakes data where organisations are of different levels of security posture.

In addition, Python simulation was practical and clear. All the data generation and analysis pipeline was created with open-source software, including pandas, random, matplotlib, and seaborn libraries, which made the logic rules flexibly testable, allowed visual consequences to be obtained in a short amount of time, and led to the generation of the results that can be duplicated without errors [7]. Notably, the simulation was also performed in real-time and made sure that access decisions could be calculated within a few milliseconds implying that the framework can be implemented into live ERP or SCM systems without considerable latency and disruption.

Nevertheless, the framework is limited. To begin with, the current detection logic is rule-based and may not become very generalizing in extremely complex or changing environments. Practically, the malicious user can evolve their request accordingly to counter the trivial policy checks [19]. This will leave a window of incorporating machine learning model or anomaly detection algorithms into subsequent versions of the product so that the machine can learn more on access patterns and adapt the detection logic accordingly. Second, the supplied simulated dataset reflected typical situations but in actual practice, the supply chains can be associated with richer contexts (e.g., location hierarchies, device metadata, dynamic workflows), which are not reflected in the modern testbed [13].

From an integration point of view, the framework acts as an external decision engine with standardized APIs to operate with ERP or SCM platforms. This will guarantee few disruption to legacy systems along with modular deployment. Gradual adoption: such architecture allows organizations to adopt the framework gradually, enabling them to implement the infrastructure in soft, monitoring or shadowing mode and then optionally follow up to hard enforcement of access control.

In a nutshell, the outcomes confirm the main principles of the framework design: dynamic evaluation of the rules, context-sensitivity, and fluidity of the integration. It has robust chances of being integrated into the real supply chain since it could accurately identify breaches, react to the anomalies in the behaviour, and is lightweight [5]. Improvements in the future can centre around testing of

adaptive policy learning and real-world implementation in sandboxed ERP systems, to determine its working capacity.

7. Conclusion and Recommendations

The paper proposed a privacy-conscious access control model that is applicable to collaborative supply chain system that recognizes the increasing requirement of protection of sensitive data in dynamic and context-aware ways. With a 1,000-synthetic-access-logs Python-based simulation, the framework was proven to be highly efficient in detecting instances of policy infringement and suspicious activity by achieving a compliance rate of 93.3 and detecting all infringements simulated [1]. This provides a smooth integration option, as the change is based on the system architecture that integrates with other platforms, such as ERP or SCM, due to the presence of application programming interfaces, and will not interfere with the current workflow [2].

Despite the accuracy of the framework, it showed a level of false positives so there is a need to have it tuned or combined with machine-learning in order to enhance its flexibility. The ideas under the improvement are focused on behaviour-sensitive learning algorithms and sandboxed desktops within enterprise [24]. Moreover, the data may be extended to have sufficient richness and features in the form of more demanding roles, access patterns, and contextual metadata can be introduced. In a nutshell, the framework is a flexible and viable framework to enforce privacy of data in the online and networked supply chain.

References

[1] A. Al-Abassi, H. Karimipour, A. Dehghantanha and R. M. Parizi, "An Ensemble Deep Learning-Based Cyber-Attack Detection in Industrial Control System," IEEE Access, Vol. 8, pp. 83965-83973,2020. https://doi.org/10.1109/access.2020.2992249.

[2] A. Alkhresheh, K. Elgazzar and H. S. Hassanein, "DACIoT: Dynamic Access Control Framework for IoT deployments," IEEE Internet of Things Journal, Vol. 1, pp. 1-1, 2020. https://doi.org/10.1109/jiot.2020.3002709.

[3] J. J. Hathaliya and S. Tanwar, "Intelligent privacy-preserving data management framework for medicine supply chain system," Security and Privacy, Vol. 1, pp. 1-15, 2024.

[4] J. A. Khan, "Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC)," IGI Global, Vol. 1, pp. 1-25, 2024.

[5] M. Aftab, Z. Qin, A. Zakria, S. Pirah and J. Khan, "The Evaluation and Comparative Analysis of Role Based Access Control and Attribute Based Access Control Model," IEEE Xplore, Vol. 1, pp. 1-8, 2018.

[6] S. Ameer, J. Benson and R. Sandhu, "An Attribute-Based Approach toward a Secured Smart-Home IoT Access Control and a Comparison with a Role-Based Approach," Information, Vol. 13, No. 2, pp. 60-60, 2022.

[7] L. Bader, J. Pennekamp, E. Thevaraj, M. Spiß, S. S. Kanhere and K. Wehrle, "Reputation Systems for Supply Chains: The Challenge of Achieving Privacy Preservation," Springer, Vol. 1, pp. 464-475, 2024.

[8] S. Berninger, S. Y. Kim, J. Piel, M. Perau, S. Geisler, F. Piller, K. Wehrle and J. Pennekamp, "Privacy-Aware Supply Chain Ratings: Interdisciplinary Research On Collaborative Supply Chain Management," Conference on Production Systems and Logistics, Vol. 1, pp. 1-15, 2025.

[9] C. Lin, D. He, X. Huang, K. K. R. Choo and A. V. Vasilakos, "BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," Journal of Network and Computer Applications, Vol. 116, pp. 42-52, 2018.

[10] M. T. Oliveira, G. R. Carrara, N. C. Fernandes, C. V. N. Albuquerque, R. C. Carrano, D. S. V. Medeiros and D. M. F. Mattos, "Towards a Performance Evaluation of Private Blockchain Frameworks using a Realistic Workload," IEEE, Vol. 1, pp. 1-8, 2019.

[11] T. Saranya, S. Sridevi, C. Deisy, T. D. Chung and M. K. A. A. Khan, "Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review," Procedia Computer Science, Vol. 171, pp. 1251-1260, 2020.
[12] S. Dey and S. Kumar, "Fostering Information Sharing Willingness: An Organizational Privacy Calculus for Industry 4.0 Supply Chains," Journal of Organizational Computing and Electronic Commerce, Vol. 34, No. 4, pp. 370-399, 2024.
[13] E. Sabbarwal and D. S. Pandey, "Data Privacy Preserving in Cloud ERP using Cryptographic Algorithm with IoT," IEEE, Vol. 1, pp. 1-7, 2024.
[14] S. Linsner, "Privacy Preserving Data Management," Springer eBooks, Vol. 1, pp. 1-300, 2025.
[15] T. Zare-Garizy, G. Fridgen and L. Wederhake, "A Privacy Preserving Approach to Collaborative Systemic Risk Identification: The Use-Case of Supply Chain Networks," Security and Communication Networks, Vol. 1, pp. 1-18, 2018.
[16] M. Uddin, "A Dynamic Access Control Model Using Authorising Workflow and Task-Role-Based Access Control," IEEE Journals & Magazine, Vol. 1, pp. 1-8, 2019.
[17] J. Sutduean, A. Singsa, T. Sriyakul and K. Jermsittiparsert, "Supply Chain Integration, Enterprise Resource Planning, and Organizational Performance: The Enterprise Resource Planning Implementation Approach," Journal of Computational and Theoretical Nanoscience, Vol. 16, No. 7, pp. 2975-2981, 2019.
[18] P. Oghazi, F. F. Rad, S. Karlsson and D. Haftor, "RFID and ERP systems in supply chain management," European Journal of Management and Business Economics, Vol. 27, No. 2, pp. 171-182, 2018.
[19] E. Kamel and A. M. Memari, "Review of BIM's application in energy simulation: Tools, issues, and solutions," Automation in Construction, Vol. 97, pp. 164-180, 2019.
[20] Q. Sun, T. C. Berkelbach, N. S. Blunt, G. H. Booth, S. Guo, Z. Li, J. Liu, J. D. McClain, E. R. Sayfutyarova, S. Sharma, S. Wouters and G. K. Chan, "PySCF: the Python-based simulations of chemistry framework," WIREs Computational Molecular Science, Vol. 8, No. 1, pp. 1-15, 2017.
[21] J. Liu, "Simulus: Easy Breezy Simulation in Python," IEEE, Vol. 1, pp. 1-8, 2020.
[22] M. Peyman, P. Copado, J. Panadero, A. A. Juan and M. Dehghanimohammadabadi, "A Tutorial on how to Connect Python with Different Simulation Software to Develop Rich Simheuristics," IEEE Xplore, Vol. 1, pp. 1-8, 2021.
[23] F. Gilson, M. Galster and F. Georis, "Generating Use Case Scenarios from User Stories," Proceedings of the International Conference on Software and System Processes, Vol. 1, pp. 1-8, 2020.
[24] F. Gilson and C. Irwin, "From User Stories to Use Case Scenarios towards a Generative Approach," IEEE Xplore, Vol. 1, pp. 1-8, 2018.
[25] C. Wang, F. Pastore, A. Goknil and L. Briand, "Automatic Generation of Acceptance Test Cases from Use Case Specifications: an NLP-based Approach," IEEE Transactions on Software Engineering, Vol. 1, pp. 1-15, 2020.
[26] A. Arabsorkhi and F. Ghaffari, "Security Metrics: Principles and Security Assessment Methods," IEEE, Vol. 1, pp. 305-310, 2018.
[27] I. Wagner and D. Eckhoff, "Technical Privacy Metrics: a Systematic Survey," ACM Computing Surveys, Vol. 51, No. 3, pp. 1-38, 2018.
[28] P. Praitheeshan, L. Pan, J. Yu, J. Liu and R. Doss, "Security Analysis Methods on Ethereum Smart Contract Vulnerabilities: A Survey," arXiv, Vol. 1, pp. 1-25, 2020.
[29] O. Novo, "Scalable Access Management in IoT using Blockchain: a Performance Evaluation," IEEE Internet of Things Journal, Vol. 1, pp. 1-15, 2018.
[30] N. Metoui, A. Alessandro, P. Prof, A. Samarati and M. Bezzi, "Privacy-Aware Risk-Based Access Control Systems," Core, Vol. 1, pp. 1-25, 2018.

[31] S. A. Sarna, M. Imran and R. Md, "Balancing Data Accessibility and Security in Cloud-Based Business Intelligence Systems," Repository Universitas Muhammadiyah Sidoarjo, Vol. 1, pp. 1-15, 2024.
[32] Kunwar, F.B., Chib, S., Tripathi, N. et al. (2025). Hybrid deep learning-driven smart energy management framework in high-tech cities using Lenet, GRU and AJFO. International Journal of Information Technology. (Springer Scopus Q2) https://doi.org/10.1007/s41870-025-02720-9
[33] Hole, Y., Hole S., L. P. Leonardo Cavaliere, B. Nair, M. Hasyim and H. B. Bapat, (2023). "Blockchain Usages in Hospitality Management," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2023, pp. 2798-2801, doi: 10.1109/ICACITE57410.2023.10183291.