Ontology-Based Access Control for Industrial Smart Vehicles

Shubodaya Heggur Narendra Kumar

Varun Shiva Prasad

Sashwath Prasad Ragothaman

Abstract— **As industrial smart vehicles develop quickly, securing the integration of complex IT systems becomes increasingly difficult. The dynamic and intricate operating environments of these vehicles frequently makes traditional access control systems inadequate. A possible approach is provided by Ontology-Based Access Control (OBAC) systems, which use formal knowledge representations called ontologies to dynamically manage and adjust access rules. By offering adaptable, safe, and context-aware mechanisms that react quickly to shifting operating environments and security threats, these systems improve security. The implementation of OBAC in industrial smart vehicle systems is examined in this research, with a focus on how it might change security procedures. OBAC ensures operational efficiency and data interoperability while supporting strong defence mechanisms against cyber threats through the integration of extensive data classifications into access control systems. In order to ensure improved security and system integrity in complicated industrial settings, the discussion aims to promote the development of advanced access control systems that are in line with the changing needs of industrial vehicles.**

I. INTRODUCTION

In the quickly developing field of industrial smart vehicles, which includes a wide range of applications from logistics and transportation to autonomous operations in different industrial environments, the incorporation of cutting-edge IT technologies has both brought in a new era of advancement and presented formidable challenges. The most important of them is the necessity of strong access control and security, which is made more necessary by the possibility of cyberattacks and illegal data access. More intelligent and adaptive solutions are required in such dynamic and highly networked situations, where traditional security measures frequently prove ineffective. By utilizing ontologies—structured frameworks that provide comprehensive definitions of data types, relationships, and categories— OBAC systems offer a promising solution to these problems. They provide flexible, context-aware access control mechanisms that can dynamically adapt to changes in vehicle operations and interactions within an industrial setting. This flexibility is necessary to quickly respond to changing conditions and security threats. The difficulty lies not only in putting in place robust security measures that can fight off dangers like information leaks and network intrusions [6], but also in making sure that these protections maintain the data interoperability and operational effectiveness that are vital to industrial smart vehicles. These vehicles need to work together and exchange data with other machinery and infrastructure in a smooth manner while maintaining system integrity and data privacy.

Recent research has offered a variety of frameworks for integrating ontology-based systems to enhance security and control over access. Can et al. [4] highlight the value of personalization while extending the possibilities of OBAC systems. They look at how finely customized access controls made possible by user-specific data integration improve operational effectiveness and security in industrial smart vehicle settings. Gupta et al. [1] on the other hand, concentrate on an attribute-based access control [8] model created especially for industrial smart vehicles that are connected to the cloud. They emphasize how access controls are dynamically assigned based on real-time assessments of vehicle and environmental factors, enhancing security without sacrificing system performance. Furthermore, Brewster et al. [2] introduce an ontology-based framework that greatly improves data reusability while maintaining strict data privacy safeguards in order to fulfil the need for precise access control that complies with the FAIR data principles. Similarly, Kim and Choi [3] show how OBAC systems can manage access controls in response to detected threats by developing an intelligent framework that identifies security contexts by analysing vulnerabilities specific to power systems, a domain sharing several characteristics with industrial smart vehicles. The insights of Chukkapalli et al. [5], who provide an ontology for smart farming within the context of attribute-based access control, further highlight the difficulty. Their research emphasizes how important safe ecosystems are for smart agriculture, an industry that depends more and more on cyber-physical systems and is therefore vulnerable to cyberattacks. The security requirements of industrial smart vehicles are similar to the focus on secure data access in smart farming. Furthermore, the theoretical underpinnings of OBAC systems are provided by Sandhu and Samarati's [6] discussion of access control fundamentals and Jin, Krishnan, and Sandhu's [9] unified attribute-based access control model, which includes DAC, MAC, and RBAC [7], provide a theoretical foundation for the effective application of OBAC in practice, emphasizing the need for organizing access control policies in a way that is reliable, adaptable, and based on accepted security practices.

Our contribution to this research is to design an access control system that supports industrial smart vehicle's function in larger industrial systems and smart environments while also meeting their specific security concerns. We want to contribute to this industry by investigating and improving OBAC systems, making sure that the security, effectiveness, and flexibility needs of industrial smart vehicle systems are properly satisfied.

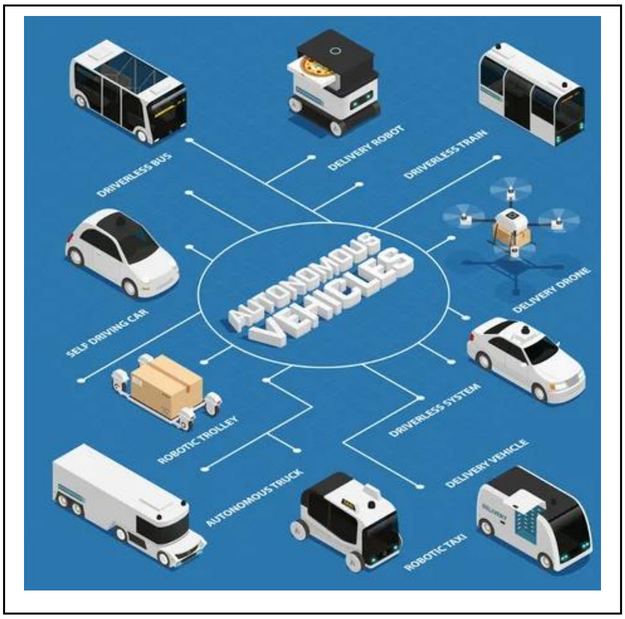

Fig1. Autonomous Vehicles and Industry [10]

II. DETAILED REVIEW OF RELATED LITRATURE

This section discusses related papers which are recently published, i.e., Gupta et al [1], Brewster et al [2], Kim and Choi [3], and Özgü Can et al [4]. Including problem solution, five advantages and disadvantages.

A. *An Attribute-Based Access Control for Cloud Enabled Industrial Smart Vehicles [1]*

Problem Solution

Important security and privacy concerns are covered in the work by Gupta et al. about the Industrial Internet of Vehicles (IIoV), specifically with regard to intelligent transportation systems (ITS). The main issue addressed is the large attack surfaces present in smart cars, which adversaries might take advantage of to compromise vital vehicle components like the engine and brakes. The authors suggest a formal Attribute-Based Access Control (ABAC) model called ITS-ABAC to address this issue. It is intended to handle individual privacy preferences and apply fine-grained security policies in an industrial ITS environment that is helped by the cloud.

Advantages

1. Enhanced Security and Privacy: By permitting only permitted communications between smart cars and infrastructure, ITS-ABAC's innovative approach to dynamic group assignment based on parameters like location, direction, and speed improves security and privacy.

2. Flexibility and Scalability: The model is very flexible and scalable to various ITS operational scenarios due to its capacity to manage changing attributes dynamically.

3. Decreased Administrative Overhead: The system makes it easier to handle access controls by utilizing groups that can inherit attributes, which lowers the administrative overhead brought on by frequent changes in the environment.

4. Compatibility with Cloud Platforms: The system's ability to work with cloud platforms such as Amazon Web Services (AWS) indicates that it is practically applicable and ready to be integrated into current cloud-based infrastructures.

5. Performance Validation: Several performance assessments are included in the article, which shows that the system has no effect on cloud-assisted operations and does not impair the performance of smart car operations.

Disadvantages

1. Complexity of Deployment: Putting in place such a sophisticated access control system may be difficult and need a high level of technical know-how, which may be prohibitive for businesses with few IT resources.

2. Possibility of Policy Misconfiguration: Because the control policies are fine-grained, there is a chance that they will be configured incorrectly, which could unintentionally allow access to unauthorized parties or prevent it from allowed ones.

3. Dependency on Precise Attribute Scheduling: The precise provisioning of qualities is critical to the system's effectiveness. Any mistakes in the attribute data may result in incorrect access decisions, which could jeopardize security.

Justification

The ITS-ABAC model, developed by Gupta et al., addresses particular issues with access control in a dispersed and dynamic context, which represents a major advancement in cloud-assisted ITS security. By incorporating group dynamics into attribute-based access control, a strong framework that can adapt to the constantly shifting circumstances seen in smart transportation systems is introduced. On the other hand, the demands of precise attribute management and their intricacy draw attention to certain areas that need close attention throughout deployment and operation.

B. *Ontology-based Access Control for FAIR Data [2]*

Problem Solution

The problem of secure, fine-grained access to FAIR (Findable, Accessible, Interoperable, Reusable) data is addressed in the study by Christopher Brewster and colleagues. The primary issue raised by the FAIR principles is the requirement for restricted access to sensitive data, especially when handling information that could have an impact on privacy, security, or competition. They suggest an OBAC system that defines access controls according to the metadata of the data and the users themselves by using domain-specific ontologies. With this method, access to data can be dynamically regulated and customized based on the user's credentials and the particular linguistic context of the requested material.

Advantages

1. Fine-Grained Access Control: Based on the semantic interpretation of data, OBAC enables very granular permission assignment, providing precise control over data access.

2. Enhanced Security and Privacy: The system makes sure that data can only be accessed by authorized users, boosting security and protecting privacy, by establishing an access control system based on metadata and ontologies.

3. Flexibility and Scalability: The system is made extremely flexible and scalable by the use of ontologies, since modifications to the ontology can handle additions of new data kinds and categories or changes in rules without requiring a complete redesign of the access control system.

4. Compliance with FAIR Principles: By enabling data access under certain circumstances and interoperability via the usage of shared ontologies, the system directly supports the FAIR principles.

5. Proof of Concept Application: The implementation, which makes use of AuthzForce and the SPARQL server Apache Jena Fuseki, illustrates the usefulness of OBAC and how it can be incorporated into current systems.

Disadvantages

1. Complexity in System Implementation and Maintenance: Keeping up-to-date ontologies and metadata can make system implementation and continuous maintenance more difficult.

2. Dependency on Accurate Metadata: The system's performance is largely dependent on the quality and accuracy of its metadata, which can be difficult to maintain in dynamic contexts where data is updated often.

3. Possible Problems with Performance: Performance bottlenecks may result from the use of ontology-based judgments and fine-grained access control, particularly with big datasets and intricate queries.

4. Learning Curve and Usability: The ontology-based system may have a substantial learning curve that makes it difficult for non-technical people to grasp and utilize.

5. Limited Real-World Testing: Although a proof of concept is given, there may be unanticipated difficulties in the real-world application, particularly in settings with highly heterogeneous data and a variety of user requirements.

Justification

Brewster et al.'s OBAC system tackles important issues with FAIR data management, particularly in sensitive domains like law enforcement and health data. The system's integration of access control with ontologies not only improves security and privacy, but also complies with the FAIR principle's more general goals. On the other hand, the intricacy of ontology management and the reliance on high-quality information are possible obstacles that may hinder the system's scalability and usefulness in a variety of settings. It is advised to conduct additional testing and development to guarantee robustness and effectiveness in a range of operational scenarios.

C. Intelligent Access Control Design for Security in Smart Grids [3]

Problem Solution

A solution to the growing vulnerabilities in the smart grid environment brought on by a variety of sophisticated cyberattacks is presented in the study by Hyoungju Kim and Junho Choi. The smart grid confronts a number of risks, including information leakage and internal system intrusions, given its integration with cutting-edge technologies like cloud computing and the Internet of Things. To improve the security management of power systems, the authors provide an intelligent access control framework that can perform dynamic and partial delegation with authorization role boundaries. Because of the security context awareness built into this framework, access controls can be adjusted in real time in response to security vulnerabilities that have been examined.

Advantages

1. Enhanced Security Through Dynamic Access Control: The framework offers dynamic access control, which is essential in the quickly changing smart grid threat scenario since it can adjust to shifting roles and threats.

2. Context Awareness: Through the integration of security context awareness, the system can improve situational awareness by analysing and drawing conclusions based on real-time data, which will enable it to respond to possible threats more precisely.

3. Scalability and Flexibility: The suggested model exhibits strong scalability and adaptability for various smart grid setups and situations because it is made to operate in a collaborative smart grid environment.

4. Experimental Validation: The researchers ran tests that showed the success of the framework, achieving a 70% accuracy rate in security context ontology-based access control inference and a 72.8% attack response rate.

5. Ontology-Based Approach: In order to improve the understanding and automation of security responses in smart grids, a structured analysis and response system utilizing security context ontology is employed.

Disadvantages

1. Complicated Implementation: The framework's reliance on in-depth ontology models and real-time data analysis could make it more difficult to apply and call for a lot of knowledge and experience.
2. Dependence on Accurate Data: In large, scattered contexts such as smart grids, the system's efficacy is largely dependent on the timeliness and accuracy of the data collected.
3. Potential Overheads: The system's performance may be impacted by computational overheads brought on by the

real-time analysis and dynamic access control, especially in large-scale deployments.

4. Misconfiguration security risks: Because of the framework's complexity and dynamic nature, there is a chance that something will go wrong and create new vulnerabilities.

5. Limited Real-World Testing: Although the experimental findings show commitment, there is a lack of detailed information regarding the system's real-world application and testing in many smart grid environments, which could hinder our ability to fully understand the system's effectiveness in varied operational contexts.

Justification

Kim and Choi's intelligent access control approach, which addresses the unique difficulties of changing threat landscapes and the requirement for context-aware security solutions, makes a substantial contribution to improving security in smart grid systems. An organized reaction to security issues and a deeper understanding are made possible by the application of an ontology-based methodology. To guarantee the framework's performance and effectiveness in real-world applications, however, difficulties like implementation complexity and the requirement for precise, real-time data analysis must be carefully controlled. To fully exploit the potential of this intelligent access control system in various smart grid situations, more in-field testing and improvements are needed.

D. Personalizable Ontology-based Access Control [4]

Problem Solution

In this work, Özgü Can, Okan Bursa, and Murat Osman Ünalır discuss the difficulty of customizing access control in settings where Semantic Web technologies are dominant. Conventional access control approaches, such Role-Based Access Control (RBAC), frequently fall short of meeting the multiple requirements and intricacies of each unique user in dynamic logical configurations. In order to provide a customized approach to access control, this study presents the OBAC model, which combines domain-specific and user-specific policy management. By enabling policies to dynamically adjust based on user profiles and specific domain standards, the model improves Semantic Web security.

Advantages

1. Enhanced Personalization: A more sophisticated and user-centred approach to security is made possible by the model's usage of user profiles to generate customized access control policies.

2. Semantic Richness: The OBAC paradigm offers richer, context-aware access control decisions that effortlessly interact with the underlying ontology-driven data models by utilizing semantic technologies.

3. Dynamic Policy Management: This feature allows policy ontologies to be created, modified, and deleted on-the-fly by the system, making it easier to adjust access controls in response to evolving security threats.

4. Conflict Resolution: In contexts with complicated access control requirements, a complex process for resolving policy conflicts is incorporated. This mechanism is essential for ensuring system integrity and operational consistency.

5. Scalability: The framework's deployment in a tourism environment demonstrates how scalable it is across other domains, indicating the possibility of a broader application.

Disadvantages

1. Complexity in implementation: The implementation and management of the access control system may become more complex with the inclusion of user profiles and logical technologies.

2. Overhead: The requirement for real-time conflict resolution and the dynamic nature of policy management could result in a large amount of computing overhead, which could have an adverse effect on system performance.

3. Dependency on Complete and Accurate User Profiles: The model's reliability is largely dependent on user profiles, which might be difficult to maintain over time or in extremely dynamic contexts.

4. Possible Privacy Issues: Privacy concerns may arise from collecting and storing detailed user profiles for access control, especially if private data is not sufficiently safeguarded.

5. Resource Intensiveness: Maintaining the ontology base and policies continuously can be resource-intensive, including a significant amount of administrative work and technological expertise.

Justification

Can et al.'s OBAC approach, which combines domain-specific rules with customized, profile-based policies, represents a major step forward in the field of access control for Semantic Web applications. This strategy fits in with the semantic structure of the underlying web technologies while also improving the adaptability and success of access control methods. To fully utilize the model's potential, nevertheless, strong implementation techniques and effective management tools are needed due to the system's complexity and resource requirements. Future advancements in this field ought to concentrate on strengthening privacy safeguards and streamlining the administration of logical policies in order to allay any worries about customized access control systems.

TABLE I. LITERATURE REVIEW OVERVIEW

Paper	**Analysis**		
	Problem Solved	***Advantages***	***Disadvantages***
Gupta et al. [1]	Security for cloud-enabled industrial smart vehicles	Dynamic, scalable, reduces admin overhead	Complex deployment, potential misconfiguration
Brewster et al. [2]	Access control for FAIR data	Fine-grained control, FAIR principles compliance	Complexity, reliance on accurate metadata
Kim and Choi [3]	Security context awareness in smart grid	Contextual awareness, scalable	Policy management overhead, limited testing
Can et al. [4]	Personalization in Semantic Web access control	Policy personalization , semantic richness	Ontology management complexity, user data reliance

III. Discussion, Future Directions and Conclusions

Recent work highlights the increasing complexity and need for sophisticated access control systems to address changing security concerns, as demonstrated by the investigation of OBAC in industrial smart vehicles. More personalization and context-aware security management have been made possible by the integration of ontology-based models and semantic web technologies [1], [2], [3], [4].

A. *Lessons Learned*

Key lessons from these studies include:

1. Enhanced Personalization and Flexibility: OBAC systems show greater flexibility than more conventional models like RBAC by dynamically tailoring access controls based on contextual information and user-specific data [4].

2. Integration Challenges: Although OBAC systems offer rich conceptual capabilities, their implementation can be complicated by the requirement to handle ontologies in detail and deal with huge, dynamic data sets [3], [4].

3. Scalability and Performance Issues: Due to their high resource requirements, these systems must have powerful processing capacity and effective data handling techniques in order to operate at a level that maintains real-time capabilities, which are crucial for industrial applications [1], [4].

4. Security and Privacy Issues: As systems are more customized, they also need to handle the growing danger to user privacy and make sure strong security measures are in place to safeguard confidential data [2], [4].

B. *Future Dirctions*

Building on recent discoveries, OBAC in industrial smart cars should prioritize the following areas going forward:

1. Simplifying Ontology Management: By creating tools and processes that make ontology updates and maintenance easier, OBAC adoption may be encouraged and system adaptability can be increased [2].

2. Improving Data Privacy: To address potential vulnerabilities that could expose user data, OBAC systems need to combine advanced encryption techniques and privacy-preserving technologies [4].

3. Enhancing Scalability and Performance: The performance problems with the current OBAC systems may be reduced with research into more effective data processing methods and the incorporation of distributed computing resources [1], [3].

4. Machine Learning and AI Integration: OBAC systems can be made even more responsive and efficient by integrating artificial intelligence to predict security risks and automate policy modifications based on real-time data [3].

C. *Conclusions*

Examining OBAC systems in the context of industrial smart vehicles demonstrates a notable movement in security models toward ones that are more user-centric and adaptable, able to meet the particular difficulties presented by contemporary industrial environments. In addition to enhancing the responsiveness and granularity of access restrictions, these systems add complications that need to be controlled in order to reach their full potential. Industrial cybersecurity has a promising but difficult frontier in the integration of OBAC systems. Future developments in industrial smart vehicle applications must concentrate on simplifying and improving these system’s functionality in order to facilitate wider adoption and improved security management.

IV. Personal Contribution

1) Shubodaya H N: Conducted literature reviews on papers [1], [2], and [3], and Conclusions of the paper, encapsulating the study's key insights and outcomes.

2) Varun S: Responsible for the literature review of paper [4], participated in discussions, extracted lessons and outlined future research directions.

3) Sashwath P R: Authored the Abstract, Introduction and assisted in paper editing.

V. References

[1] M. Gupta, F. M. Awaysheh, J. Benson, M. Alazab, F. Patwa, and R. Sandhu, “An Attribute-Based Access Control for Cloud Enabled Industrial Smart Vehicles,” IEEE Transactions on Industrial Informatics, vol. 17, no. 6, pp. 4288–4297, Jun. 2021.

[2] C. Brewster, B. Nouwt, S. Raaijmakers, and J. Verhoosel, “Ontology-based Access Control for FAIR Data,” *Data Intelligence*, vol. 2, no. 1–2, pp. 66–77, Jan. 2020.

[3] H. Kim and J. Choi, “Intelligent Access Control Design for Security Context Awareness in Smart Grid,” *Sustainability*, vol. 13, no. 8, p. 4124, Apr. 2021, doi: https://doi.org/10.3390/su13084124.

[4] Ö. Can, O. Bursa, and M. O. Ünalır, "Personalizable Ontology-Based Access Control," Gazi University Journal of Science, vol. 23, no. 4, pp. 465-474, 2010.

[5] S. S. L. Chukkapalli, A. Piplai, S. Mittal, M. Gupta, and A. Joshi, “A smart-farming ontology for attribute based access control,” in Proc. 6th IEEE Int. Conf. Big Data Secur. Cloud, 2020, pp. 29–34.

[6] R. S. Sandhu and P. Samarati, “Access control: principle and practice,” IEEE Communications Magazine, vol. 32, no. 9, pp. 40–48, Sep. 1994.

[7] D. F. Ferraiolo et al., “Proposed NIST standard for role-based access control,” ACM Trans. Inf. Syst. Secur., vol. 4, no. 3, pp. 224–274, 2001.

[8] V.C.Huetal.,“Guide to attribute based access control (ABAC) definition and considerations,” NIST Publication, Gaithersburg, MD, USA, Tech. Rep. 800-162, 2014.

[9] X. Jin, R. Krishnan, and R. Sandhu, “A unified attribute-based access control model covering DAC, MAC and RBAC,” in Proc. DBSec, 2012, pp. 41–55.

[10] “Autonomous Vehicles and Industry 5.0,” www.kontron.com. https://www.kontron.com/en/blog/mobility/autonomous-vehicles-and-industry-5.0