STM JOURNALS

International Journal of
Advanced Control and
System Engineering

ISSN: 3049-1452
Volume 3, Issue 2, 2025
July–December
DOI (Journal): 10.37591/IJACSE

https://journals.stmjournals.com/ijacse

Review IJACSE

A Survey of Role-Based Access Control Implementation in HMI Systems for Industrial Automation

Alpeshkumar Kathiriya

Abstract

The convergence of role-based access control (RBAC) and human–machine interface (HMI) systems present a transformative approach to secure and efficient industrial automation in Industry 4.0. By integrating RBAC with multifactor authentication (MFA), this framework enhances cybersecurity while maintaining operational flexibility and mitigating both external threats and internal vulnerabilities. Modern adaptive HMIs further optimize the user experience through personalized and intuitive interfaces; however, challenges remain in balancing functionality with simplicity in complex industrial environments. Future research directions include AI-driven dynamic RBAC for real-time permission adjustments, blockchain-based decentralized access control, and quantum-resistant encryption for safeguarding supervisory control and data acquisition (SCADA) systems. Additionally, advancements in behavioral biometrics, predictive HMIs, and explainable AI will refine security and usability, whereas augmented reality (AR)-enabled training and energy-efficient authentication protocols will address workforce and Industrial Internet of Things (IIoT) challenges. This study highlights the critical synergy between RBAC and HMI in smart manufacturing and proposes innovative solutions to bridge the current gaps and drive next-generation industrial automation toward resilient, user-centric, and secure operations.

Keywords: Role-based access control (RBAC), human–machine interface (HMI), Industry 4.0, multifactor authentication (MFA), adaptive interfaces, industrial cybersecurity, smart manufacturing

INTRODUCTION

The shift to smart manufacturing has been facilitated by digitization, embedded technologies, and the IIoT. Cutting-edge cyber-physical manufacturing systems aim to increase productivity and efficiency. The connection between integration firms has changed noticeably as a result of the implementation of Industry 4.0 (I4.0) solutions. Consequently, companies must either build new HMIs or modify their existing ones, making intentional HMI design crucial [1]. Purposeful design focuses on human-oriented planning of HMIs that considers the specifics of the industrial context.

***Author for Correspondence**
Alpeshkumar Kathiriya
E-mail: akathiriya37@gmail.com

Independent Researcher, Application Engineer, IT Department Amneal Pharmaceuticals, Limited Liability Company, New Jersey

Received Date: July 31, 2025
Accepted Date: August 25, 2025
Published Date: October 15, 2025

Citation: Alpeshkumar Kathiriya. A Survey of Role-Based Access Control Implementation in HMI Systems for Industrial Automation. International Journal of Advanced Control and System Engineering. 2025; 3(2): 10–19p.

Data security and privacy are becoming increasingly important, as several studies have shown that financial software is particularly vulnerable to unauthorized access, which may result in significant losses. The importance of access control in ensuring the security of software and hardware resources is increasing. Role-based access control (RBAC) offers a robust solution for meeting access control requirements. A document outlining the guidelines for configuring the procedure for approving or rejecting user authorizations is known as an access control policy. At its core, RBAC revolves around the concept of roles. A role is an

authorization to execute an operation on an object, which may be an action, function, or task that a user can call upon according to the standard [2]. Objects can be either data storage devices or physical resources, such as computers, printers, and network drivers. Typically, there is a one-to-many relationship between users and sessions and a many-to-many relationship between sessions and roles. Using RBAC, a user may activate many roles in a single session; however, this is not necessary to do so. The fundamental RBAC principle, which is executed via sessions, allows many-to-many user permission assignments.

HMI is a platform that allows people and machines to communicate and share information with each other. By considering the user's motivating objectives throughout an interaction, current user experience (UX) research strives to improve usability, performance, and overall user satisfaction. Determination and confidence in one's abilities drive users to use AI. Factors inherent to these motivators should be considered by manufacturing organizations seeking to improve UX. These include the system's potential to support intuitive and quick job completion and its ability to anticipate user demands [3]. The second impacts the amount of memory needed to perform a job and is highly related to the user's cognitive ability. One definition of Adaptation is defined as the ability of systems to adjust to different user needs, circumstances, and platform capabilities. Adaptive User Interfaces (AUIs) have been integral to smart user experience design since the beginning of human-computer interfaces (HCI). Not only can AUI increase user performance, but it can also improve UX and the acceptability of usage by providing personalization, specifically designed instructions, and support.

Structure of the Paper

This study begins with an introduction outlining Industry 4.0 challenges and RBAC-HMI synergy, followed by Section II explaining the understanding of RBAC. Section III details the human–machine interaction (HMI). Section IV covers the Implementation of RBAC in HMI Systems for Industrial Automation. Section V reviews the literature using a comparative table. Section VI concludes the paper and proposes future work.

UNDERSTANDING ROLE-BASED ACCESS CONTROL

In the 1970s, Internet systems that could support many users and applications were the first to implement RBAC. RBAC's main idea of RBAC is that users are allocated to the proper roles, and permissions are linked to roles. This makes permission management much easier. A company's numerous job functions are mapped to specific roles, and users are assigned specific roles according to their duties and credentials [4]. The ability to transfer users between different roles is convenient. As more apps and systems are added, roles may be assigned new permissions, and rights can be revoked as necessary. To further obfuscate the mapping of user rights to specific permissions or privileges, the RBAC proposes an additional layer of indirection. Therefore, this mapping is divided into two parts by roles: the first portion maps users to roles, and the second half maps roles to privileges. This is shown in Figure 1.

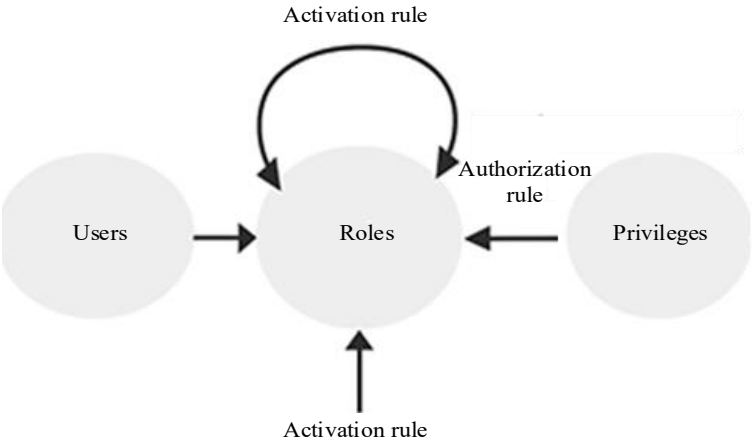

Figure 1. The basic RBAC model.

A role is best understood as a semantic concept that forms the basis of an access control policy. A role is a temporary container for a set of associated users and their rights. Due to the reduced frequency of changes in the operations or functions of an organization, the position is more stable.

The Precursors of RBAC

The sociological perspective holds that status inconsistency, which suggests many functions, is the root cause of role overload, ambiguity, and conflict precursors. Additionally, they wanted to find out when role conflict is similar to status inconsistency. In the absence of status considerations within the policy engineering context of the role engineering setting, three fundamental problems emerge: role overload, ambiguity, and conflict. These concerns initially exacerbate the difficulties in the engineering process [5]. The predecessors and their connections to the RBAC model are shown in Figure 2. Therefore, it stresses that organizational mining procedures explain these precursors in ways that uniquely enable an understanding of the connections between them. No prior research has examined the antecedent function of these components in RBAC for access control in Knowledge Management Systems (KMS), although several studies have addressed them individually or in combination across many fields. Although these words have different technical meanings in the RBAC system, they are familiar with their semantic meanings in other fields.

Integrating RBAC with Encryption for Enhanced Security

RBAC and encryption are two fundamental security mechanisms that, when integrated, provide a robust defense-in-depth approach to data protection [6, 7].

- *Complementary security layers:* RBAC regulates who can access resources by assigning permissions to roles, which are then assigned to users. Encryption secures access by protecting data confidentiality and integrity, both at rest and in transit. Together, they ensure that even if unauthorized access attempts occur, the encrypted data remains protected.

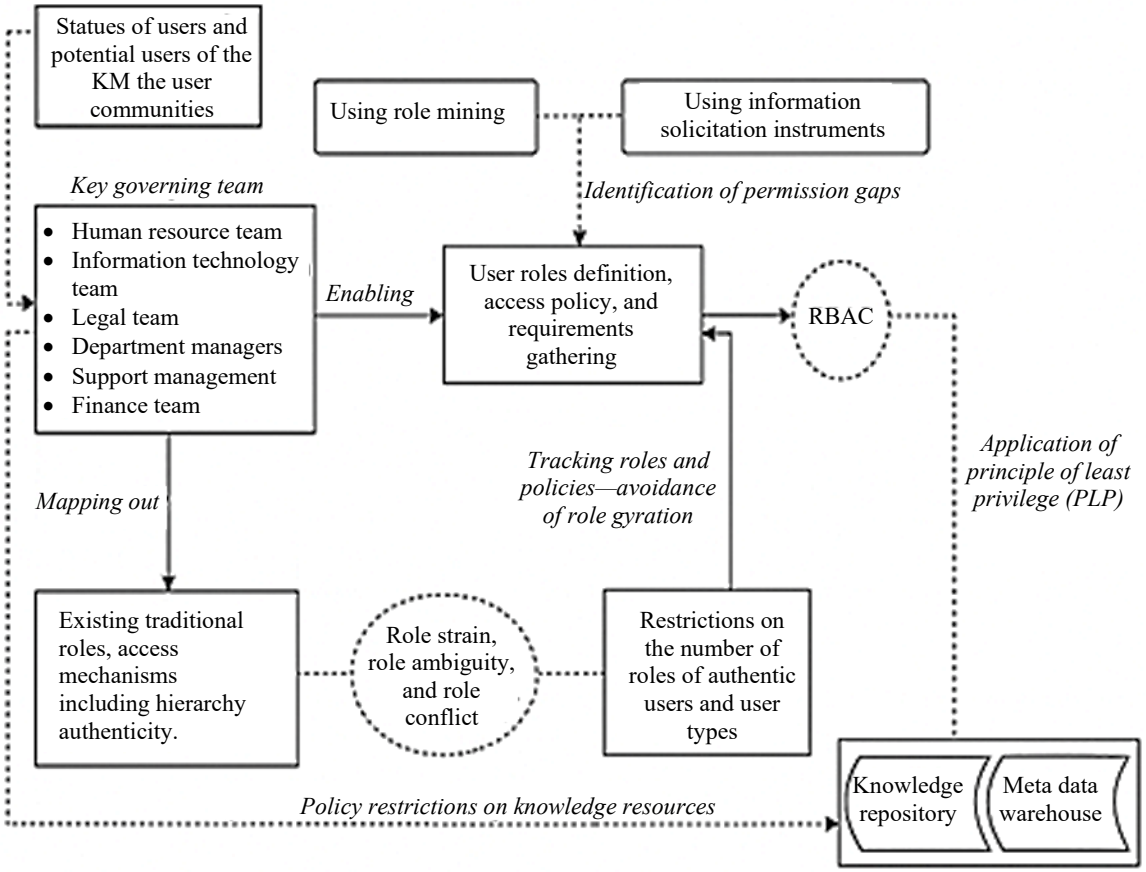

Figure 2. The precursors and their relationship with the RBAC model.

- *Minimized attack surface:* RBAC limits data access to only authorized roles, reducing the exposure of encrypted keys and ciphertexts to a smaller, controlled group. This containment significantly reduces the potential for insider threats and accidental data leaks.
- *Granular access control:* Combining RBAC with encryption enables fine-grained access policies in which encryption keys can be tied to roles rather than individual users. This simplifies management and ensures that users gain decryption rights strictly according to their role permissions.
- *Improved compliance and auditability:* Many regulations (e.g., GDPR and HIPAA) mandate strict access controls and data encryption. Integrated RBAC and encryption systems provide clear audit trails showing both access authorization and cryptographic protection, thereby easing compliance efforts.
- *Resilience against data breaches:* Even if attackers bypass RBAC controls, encrypted data remains unintelligible without the correct cryptographic keys, enhancing the overall system resilience.

HUMAN–MACHINE INTERACTION

The evolution of computers and other machines brought about the automatic representation of the term HCI, which may refer to either Man-Machine Interaction or Man-Machine Interfacing. It is rather clear that complicated machines are not useful unless humans know how to utilize them [8]. This simple argument presents the two most important terms that should be considered while building an HCI: usability and utility. Finally, the reason for a system's development may be uncovered by examining its capabilities, or more precisely, how its functions contribute to the achievement of its aim. The functionality of a system is defined by the variety of activities or services it provides to its users. Conversely, functionality is only valuable if it is easy for the user to use [9]. The usability of a system is defined as the degree to which its features may be appropriately and successfully used to accomplish the goals of the individual users. When the practicality and efficiency of a system are well coordinated, it can perform its intended tasks.

Except for a few third-party component integration choices, such as ActiveX.NET and Windows Presentation Foundation (WPF) controls, the process of HMI creation is still predicated on a rather limited collection of tools and predefined objects [10]. Additionally, because of their restricted interchangeability across other supervisory control and data acquisition (SCADA) systems, these components provide only a partial solution to the issue. The graphic designer of the HMI only has access to a limited range of control components; therefore, users of these systems cannot fully utilize the sophisticated visualization tools and processes at their disposal.

Authentication Methods in Human–Machine Interaction

The authorization mechanism in the HMI plays an important role in guaranteeing secure and reliable communication. Traditionally relying on users and passwords, authentication has advanced to include complex methods such as biometric verification, finger marks, face identification, and sound authentication [11].

- *Passwords and PINs:* Authentication techniques in HMI initially start with traditional methods such as passcodes and PINS. Despite being simple, these passcodes and PINS are likely to be popular owing to their ease of administration and familiarity to users.
- *Biometric authentication:* Biometric authentication is an advance in HMI security, transforming old-fashioned methods of confirming user identities. Utilizing unique physical or behavioral properties, such as fingerprints, facial expressions, or speech patterns, biometric verification boosts the accuracy and security of user identification.
- *Multifactor authentication multiplicative-factoring formalization* (MFF) is an important aspect of HMI security that presents a further level of security beyond the usual methods. In MFF, users must confirm their identity using a blend of aspects, such as something they remember (similar to a passcode), something they possess, and something they are (such as biometric features).

Supervisory Control and Data Acquisition

Figure 3 shows an example of a SCADA system. Such systems are used to regulate, monitor, and acquire data from various processes, including those involved in manufacturing, power generation, and other similar endeavors [12]. The SCADA system performs four tasks: data collection, network connection, data display, and control and monitoring. To function, SCADA relies on four primary parts:

- A programmable logic controller (PLC) is a data collection instrument that can learn about the present state of the operating system via input and output devices, including temperature, air pressure, count, and other similar sensors.
- A PLC serves as a remote telemetry unit (RTU), a computer that gathers data from sensors and transmits it to a SCADA master or an HMI. The RTU converts the digital or analog signals from the sensors to signals that may be delivered to the SCADA master, depending on the protocol.
- A SCADA master/HMI that allows users to engage in direct system-to-user data control, monitoring, and acquisition is used.
- The communication network links RTUs with SCADA Masters via an RS232 connection [12].

Working at SCADA

SCADA systems include data gathering and telemetries. Gathering data, sending it back to the main unit, performing any necessary examinations and controls, and finally displaying the data on multiple operator screens are all components of SCADA. The process is then informed by the required control tasks. There are four main components to the SCADA concept of operation:

- Data acquisition
- Networked data communication
- Data presentation
- Control

These functions are elaborated as follows.

In industrial systems, where constant monitoring is required, many types of sensors are installed at various locations. These sensors can measure pressure, temperature, Hall effect, and other parameters. The microcontroller receives readings from the sensors, which continuously measure the different parameters. These locations depend on accurate plant operation and regular evaluation; however, human intervention poses serious unintentional risks and results in operating losses. Instead of using human monitoring to address this, sensors are placed at key locations.

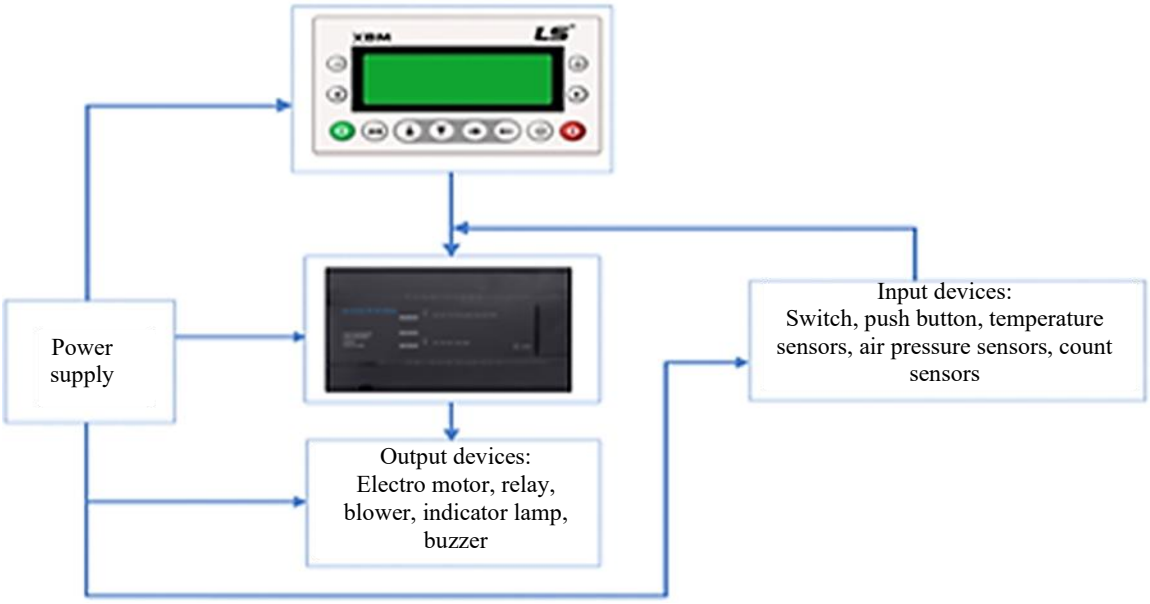

Figure 3. Block diagram of SCADA systems.

A general-purpose microcontroller board has a microcontroller attached to it. Based on the inputs it receives, it applies the appropriate algorithm to translate the readings into standard units. Additionally, the microcontroller board is linked to wireless network protocols, including Bluetooth, ZigBee, GSM, and the Internet. These provide efficient data transfer to the central control unit from distant locations. The data are shown on a computer screen at the receiving end, where human supervision is applied, allowing the operation of remote components of the industrial unit from a central location. In the case of an abnormality, the system promptly notifies the supervisor to prevent operational and financial losses.

IMPLEMENTATION OF RBAC IN HMI SYSTEMS FOR INDUSTRIAL AUTOMATION

The centralized RBAC model illustrates the overall architecture of the proposed system. There are five subsystems that make up the overall architecture of the proposal: the client, the Multimodal Biometric Authentication Processing System (MBAPS) handler, the AC module, and the Roles Database. The three subsystems that make up the server are the AC module, Modbus Application Protocol (MBAP) Shandler, and MBAP handler. The abbreviation for "Modbus Application Protocol Secure" is MBAPS. A detailed explanation of the interplay between these entities is provided below as part of their proposal. SCADA systems are examples of clients that are subsystems that pose connection requests [13]. The entity or sub-system responsible for establishing a secure connection with the client, with which the MBAPS must communicate directly. It receives the client's request for a secure connection and authenticates it using a certificate as part of the Transport Layer Security (TLS) mutual authentication process. The MBAPS handler transfers the Modbus frame to the MBAP handler after establishing a secure connection and authorizing it. Therefore, this component is involved in authentication and authorization procedures. The AC module is responsible for implementing the policies that have been discovered in the role database by performing the relevant verifications. The AC module has limited interactions with entities other than the role database because it receives its trigger to execute its operations from the MBAPS handler module.

Traditional RBAC

The RBAC approach introduces the notion of a role to logically separate users and permissions. Subsequently, each user may be assigned a role that grants them access to the system, thereby allowing them to access the information system. In the classic RBAC paradigm, there is a many-to-many link between roles and users. Every user needs a role or roles, and a role might have more than one set of permissions [14]. Additionally, there is a many-to-many link between privileges and positions in the hierarchy. The users were the people shown in Figure 4 who had access to the system. The system is accessible only to authorized personnel. Users symbolize the collection of the users. The role separates the interactions between users and permissions by acting as an intermediary layer between the two. To link the privilege set in RBAC, a role is used rather than a User or a Group. A position in a company is the most typical definition of a role. Roles stand in for role sets. A user-created notion is that a session is dynamic. An individual user may engage in a collection of system-related responsibilities during a session. The sessions stand for the session set. Authorization that allows a user to access a system of information is called a permission.

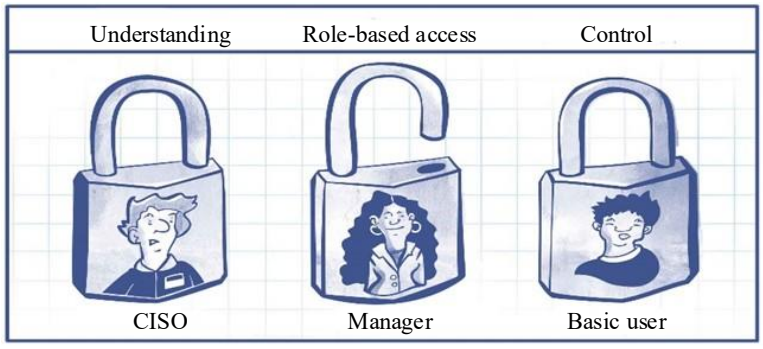

Figure 4. The definitive guide to role-based access control (RBAC) [14].

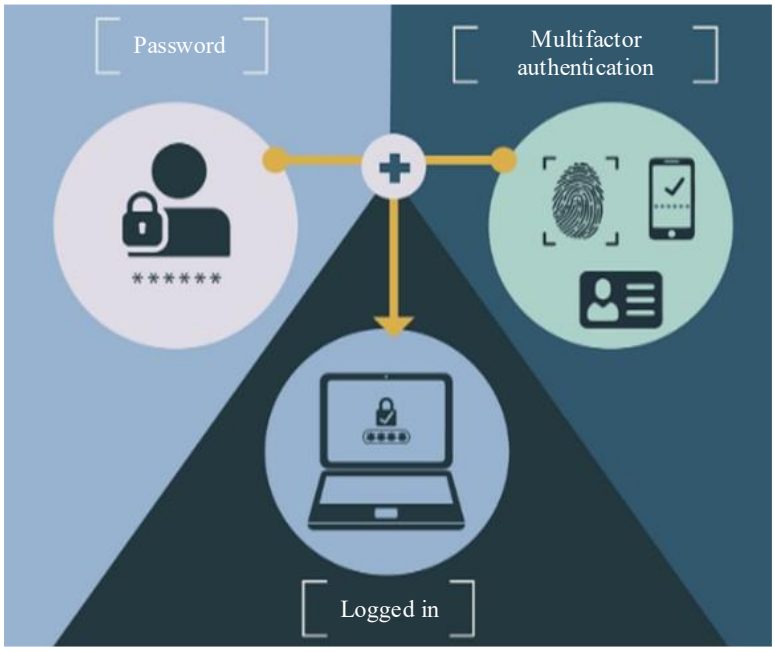

Figure 5. Multifactor authentication [15].

The RBAC approach facilitates a more realistic mapping of management practices to security rules, aligning system security management with actual application requirements. Some web applications may benefit from the increased security of the RBAC model because of its adaptability in controlling the overall security policy of the application system.

Multifactor Authentication

The use of multifactor authentication (MFA) to confirm a user's identity before allowing access to restricted content is on the rise across online businesses [15]. Figure 5 shows that MFA adds an extra layer of security to typical login credentials by requiring the user to input a code or piece of data that they own. MFA requires a minimum of two authentication methods from the user.

The authentication methods used are as follows:

- Something the user has
- Something the user knows
- Something the user is.

The MFA framework was created to improve system security and make it easier to keep computers and systems safe from unwanted access. Possession, knowledge, and uniqueness are the three authentication mechanisms necessary for constructing an MFA system [16]. As an extra layer of security, MFA architecture often employs biometrics in addition to login and password authentication. According to professionals in the field, text passwords, OTPs, and two-factor combinations are the most popular authentication methods and strategies. The main reason for their selection was their suitability for the application being developed.

Limitations and Challenges in RBAC and HMI

Reaching the rights linked to a certain function may be challenging. The exclusive right to change roles allows the deletion or modification of permissions associated with each position [17]. Despite job roles being assigned based on the bare minimum power, a user's role shift may cause difficulty when considering the rights of each person involved.

Striking a balance between providing extensive capabilities and preserving an intuitive interface is one of the biggest challenges in human–machine interface design. The goal of many features included in

today's automobiles is to make driving more enjoyable, and these features range from voice assistants and gesture controllers to highly customizable displays. However, too many capabilities may be overwhelming, especially for those who are not accustomed to cutting-edge technology [18]. Prioritizing key elements and arranging them to allow rapid and simple access while reducing cognitive load are important tasks for designers. Furthermore, a precise understanding of the intentions and behaviors of people and vehicles is crucial.

LITERATURE REVIEW

Research has identified several new directions at the nexus of security systems, AI, and human–machine interaction. In the field of reinforcement learning for human–robot interaction, it has been demonstrated that assistive robots can function differently for users with diverse physical attributes, such as waist circumference. These differences may result from intrinsic task characteristics that make relying on physical traits for aid more challenging, in addition to representation bias during training [19].

Building on this, surgeons can now kinesthetically train robotic arms for sensitive tasks, such as navigating and using neuroendoscopes, thanks to advancements in robot learning. Surgeons can guarantee safe and effective performance within the limitations of the surgical environment by using task demonstrations, real-time corrections, and preference instructions. These advancements show how collaborative human-AI systems can improve processes while upholding crucial ethical standards, establishing a mutually beneficial relationship in which AI complements human capabilities rather than replacing them [20].

Comparable prospects are being investigated in industrial settings. Human–machine interaction is essential for maximizing efficiency, guaranteeing safety, and spurring innovation in the electric vehicle battery industry. The effectiveness and adaptability of industrial systems are further improved by user-centric design methodologies that incorporate data-driven optimization, usability assessment, and ongoing operator behavior modification [21].

Applications with a security focus also highlight the benefits of integrating cutting-edge technology and human supervision. For example, biometric-based RBAC systems have been successfully implemented with rigorous performance indicators, such as false acceptance and denial rates, quick authentication, and real-time monitoring. Secure blockchain wallet architectures with MFA and thorough system modeling have been created for digital asset management to improve cryptographic key security and expedite validation procedures [22].

An approach that combines user-centric design with usability testing, data-driven optimization, and continuous tuning in response to user activity is suggested. This seeks to improve the user experience in industrial systems by designing effective, efficient, and adaptable HMIs. An RBAC system that incorporates biometric authentication (fingerprints) and authorized security monitoring and control software keeps tabs on breaches in real time. Using a distributed access control system, the BioLite N2 was mounted on the room door and linked to the server. The following were included in the trial and testing: system operation, biometric reading speed, role access, FAR, FRR, and monitoring [23].

The goal of this study is to improve digital asset management and cryptographic keys by incorporating four distinct MFA settings into a secure blockchain wallet website implementation. A thorough system model was created to adequately comprehend the architecture of the system and visualize its relationships. In addition, the solution was tested and evaluated extensively after construction using Python and Ethereum libraries. According to the findings, system models improve and ease blockchain wallet installation and validation, which helps create strong security measures [24].

A functioning wind farm provided data used to evaluate the framework, with past stoppages accurately identified using alarm data. For testing, a random forest algorithm and bagging were used, together with

100 iterations of a base learner in a 10-fold cross-validation technique. A total of 95.8% of instances were correctly identified using the proposed framework, with only 4.16% of cases misclassified. The feasibility of utilizing SCADA data to predict wind turbine breakdowns using Machine Learning (ML) algorithms is demonstrated, although it highlights the need for ongoing study and fine-tuning to maximize the performance of the models [25, 26].

CONCLUSION AND FUTURE WORK

The integration of RBAC with HMI systems offers a robust solution for secure and efficient industrial automation in Industry 4.0, combining structured permission management with enhanced security through MFA to mitigate external and internal threats. Although adaptive HMIs improve the user experience through personalization and intuitive design, challenges persist in balancing functionality with simplicity and addressing evolving cybersecurity risks. Future advancements should focus on intelligent, context-aware access control, advanced authentication methods, and AI-driven interface personalization to strengthen the security and usability of the system. As industrial systems become more interconnected, the synergy between RBAC and HMI will be pivotal in developing secure and user-friendly smart manufacturing environments, requiring continuous innovation to meet the demands of next-generation automation and maintain operational efficiency in increasingly complex industrial landscapes.

Future research should explore AI-driven dynamic RBAC systems that automatically adjust user permissions based on real-time behavioral patterns and contextual factors in industrial settings, while investigating the integration of blockchain technology for decentralized, tamper-proof access control logs. Advanced biometric authentication methods, including behavioral biometrics and continuous authentication systems, must be developed to enhance security without compromising HMI usability in high-risk environments. The implementation of quantum-resistant encryption protocols will become increasingly critical for protecting SCADA systems against emerging cyber threats. Further studies should focus on developing adaptive HMIs with predictive capabilities using machine learning to anticipate user needs and dynamically optimize interface layouts, particularly for complex industrial operations.

REFERENCES

1. Panter L, Leder R, Keiser D, Freitag M. Requirements for human–machine-interaction applications in production and logistics within Industry 5.0: a case study approach. Procedia Comput Sci. 2024;232:1164–1171. doi:10.1016/j.procs.2024.01.114.
2. Salunke D, Upadhyay A, Sarwade A, Marde V, Kandekar S. A survey paper on role based access control. Int J Adv Res Comput Commun Eng. 2013;2(3):1340–1342.
3. Carrera-Rivera A, Reguera-Bakhache D, Larrinaga F, Lasa G. Exploring the transformation of user interactions to adaptive human–machine interfaces. In: Proceedings of the XXIII International Conference on Human Computer Interaction (Interacción ’23). New York (NY): Association for Computing Machinery; 2024. Article 23, p. 1–7. doi:10.1145/3612783.3612807.
4. Cai W, Huang R, Hou X, Wei G, Xiao S, Chen Y. Atom-role-based access control model. IEICE Trans Inf Syst. 2012;E95-D(7):1908–1917. doi:10.1587/transinf.E95.D.1908.
5. Patel R. Security challenges in industrial communication networks: a survey on Ethernet/IP, ControlNet, and DeviceNet. Int J Recent Technol Sci Manag. 2022;7:54–63.
6. Nyame G, Qin Z. Precursors of role-based access control design in KMS: a conceptual framework. Information. 2020;11(6):334. doi:10.3390/info11060334.
7. Khan JA. Role-based access control (RBAC) and attribute-based access control (ABAC). In: Improving security, privacy, and trust in cloud computing. Hershey (PA): IGI Global Scientific Publishing; 2024. p. 113–126.
8. Jyoti K, Kaur G. Human computer interaction. Int J Multidiscip Res. 2023 Mar–Apr;5(2):1–9. doi:10.36948/ijfmr.2023.v05i02.1913.
9. Malali N, Madugula SRP. Predictive analytics and artificial intelligence for regulatory (RegTech) compliance in the financial industry. 2025 4th International Conference on Distributed Computing

and Electrical Circuits and Electronics (ICDCECE), Ballari, India. 2025. p. 1–7. doi:10.1109/ICDCECE65353.2025.11035220.
10. Šverko M, Grbac TG. Automated HMI design as a custom feature in industrial SCADA systems. Procedia Comput Sci. 2024;232:1789–1798. doi:10.1016/j.procs.2024.02.001.
11. Verma A, Chouhan APS, Singh V, Singh L, Suklabaidya G, Sharma A, Verma P. Security and privacy in human–machine interaction for healthcare. In: Subasi A, Qaisar SM, Nisar H, editors. Artificial Intelligence Applications in Healthcare and Medicine: Artificial Intelligence and Multimodal Signal Processing in Human–Machine Interaction. Cambridge (MA): Academic Press; 2025. p. 377–392. doi:10.1016/B978-0-443-29150-0.00006-8.
12. Setiawan A, Sugeng KKI, Koesoema KI, Bakhri S, Aditya J. The SCADA system using PLC and HMI to improve the effectiveness and efficiency of production processes. IOP Conf Ser Mater Sci Eng. 2019;550(1):012008. doi:10.1088/1757-899X/550/1/012008.
13. Figueroa-Lorenzo S, Añorga J, Arrizabalaga S. A role-based access control model in Modbus SCADA systems: a centralized model approach. Sensors. 2019;19:4455. doi:10.3390/s19204455.
14. Cheng YL, Wang F, Shang LM, Wang BR, Xu J. Improved access control strategy based on RBAC model and its application. Adv Comput Sci Res. 2016. doi:10.2991/iccsae-15.2016.151.
15. Williamson J, Curran K. The role of multi-factor authentication for modern day security. Semicond Sci Inf Devices. 2021;3:16–23. doi:10.30564/ssid.v3i1.3152.
16. Syahreen M, Hafizah N, Maarop N, Maslinan M. A systematic review on multi-factor authentication framework. Int J Adv Comput Sci Appl. 2024;15:1043–1050. doi:10.14569/IJACSA.2024.01505105.
17. Sunitha BS, Basu AB. Review of role based access control method for securing user space in cloud computing. Int J Comput Trends Technol. 2014 Aug;14(1):22–25.
18. Grobelna I, Mailland D, Horwat M. Design of automotive HMI: new challenges in enhancing user experience, safety, and security. Appl Sci. 2025;15(10):5572. doi:10.3390/app15105572.
19. Evans Z, Leonetti M, Brandão M. Bias and performance disparities in reinforcement learning for human–robot interaction. 2025 20th ACM/IEEE International Conference on Human-Robot Interaction (HRI), Melbourne, Australia. 2025. p. 1299–1303. doi:10.1109/HRI61500.2025.10974226.
20. Lee A, Rapoport BI. Leveraging physical human–robot interaction for surgical robot learning in neuroendoscopy. 2025 20th ACM/IEEE International Conference on Human-Robot Interaction (HRI), Melbourne, Australia. 2025. p. 1866–1868. doi:10.1109/HRI61500.2025.10973957.
21. Kytainyk VV, Yushchenko AG, Lyalin DY. AI–human cooperation in “second brain” technology as a modern implementation of general evolution in human–machine interaction. 2025 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA), Ankara, Turkiye, 2025. p. 1–9. doi:10.1109/ICHORA65333.2025.11017255.
22. Leong WY, Leong YZ, Leong WS. Human–machine interaction in the electric vehicle battery industry. 024 10th International Conference on Applied System Innovation (ICASI), Kyoto, Japan. 2024. p. 69–71. doi:10.1109/ICASI60819.2024.10547945.
23. Chauhan A, Upadhyay S. Designing user-friendly human–machine interaction interfaces for industrial systems. 2024 IEEE 13th International Conference on Communication Systems and Network Technologies (CSNT), Jabalpur, India. 2024. p. 794–801. doi: 10.1109/CSNT60213.2024.10546005.
24. Maulana N, Istiqomah F, Priananda CW. Integration of centralized fingerprint biometric authentication to prevent room access violations using RBAC. 2023 International Conference on Advanced Mechatronics, Intelligent Manufacture and Industrial Automation (ICAMIMIA), Surabaya, Indonesia. 2023. p. 905–909. doi:10.1109/ICAMIMIA60881.2023.10427918.
25. Almadani MS, Hussain FK. Implementing a secure blockchain-based wallet system with multi-factor authentication. 2023 IEEE International Conference on e-Business Engineering (ICEBE), Sydney, Australia. 2023. p. 23–30. doi:10.1109/ICEBE59045.2023.00010.
26. Verma AK, Fatima S, Panigrahi BK. A reliable framework for predicting wind turbine failures utilising SCADA and alarm data. 2023 5th International Conference on System Reliability and Safety Engineering (SRSE), Beijing, China. 2023. p. 232–237. doi:10.1109/SRSE59585.2023.10336088.

