International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 14, Issue 2, 2026

Automation Framework For Sap – Design & Implementation Of An Automated Sap User Access Management And Access Governance

Syed Nadeem Ahmed[1], Dr. Syed Asadullah Hussaini[2]

[1]PG Scholar, Department of Computer Science & Engineering, ISL Engineering College, Hyderabad, India.

[2]Associate Professor, Department of Computer Science & Engineering, ISL Engineering College, Hyderabad, India.

Mail Id;Ahm.nadeem0@gmail.com[1], drasadullah@islec.edu.in[2]

Article Received: 14-02-2026, Accepted 27-03-2026

ABSTRACT:

In modern enterprises, SAP systems play a critical role in managing business operations such as finance, logistics, human resources, and supply chain processes. As organizations grow, managing user access and ensuring proper authorization within SAP environments becomes increasingly complex. Traditional manual processes for user provisioning, role assignment, access approvals, and compliance monitoring are time-consuming, error-prone, and difficult to audit. These challenges can lead to security risks, compliance violations, and operational inefficiencies.

This project focuses on the design and implementation of an automation framework for SAP User Access Management and Access Governance to streamline and secure the management of user identities and authorizations. The proposed framework integrates automation tools, predefined workflows, and governance policies to simplify processes such as user creation, role assignment, access requests, approval workflows, and periodic access reviews. By leveraging technologies such as SAP governance tools, automated scripts, and workflow-based approval mechanisms, the framework reduces manual intervention while ensuring compliance with organizational security policies.

The system architecture includes modules for access request management, role-based access control (RBAC), segregation of duties (SoD) analysis, automated provisioning, and audit reporting. These components work together to provide a centralized and standardized approach to access governance. The automation framework also improves traceability and transparency by maintaining detailed logs and reports for auditing and compliance purposes.

Implementation of this framework significantly enhances operational efficiency, reduces administrative workload, and minimizes the risk of unauthorized access. Additionally, it supports regulatory compliance by enforcing consistent security policies and enabling real-time monitoring of user activities. The results demonstrate that automated access governance within SAP environments can improve system security, accelerate access provisioning, and provide better control over enterprise resources.

Overall, this project highlights the importance of automation in SAP security management and presents a scalable framework that organizations can adopt to strengthen access governance, improve compliance, and ensure secure management of SAP user access across enterprise systems.

Keywords—*SAP Security, User Access Management, Access Governance, Automation Framework, SAP GRC, Role-Based Access Control (RBAC), Segregation of Duties (SoD), Workflow Automation, Identity and Access Management (IAM), Compliance Management, Access Provisioning, Audit and Monitoring*

INTRODUCTION

The project titled *"Automation Framework for SAP – Design and Implementation of an Automated SAP User Access Management and Access Governance System"* focuses on developing a comprehensive and scalable automation framework to streamline SAP user access management and governance processes. The primary objective is to minimize manual intervention, enhance system security, ensure regulatory compliance, and improve overall operational efficiency in SAP system administration. The framework automates key user lifecycle activities, including user creation, role assignment, user modification, and user deactivation. New user accounts are automatically generated based on approved access requests, while roles and authorizations are assigned according to predefined job responsibilities. Similarly, any changes such as departmental transfers or role updates are handled through automated processes, and user access is promptly revoked or locked when employees exit the organization or change roles, thereby reducing the risk of unauthorized access [1], [2].

Furthermore, the framework integrates seamlessly with governance and compliance tools such as SAP

DOI: https://doi.org/10.62647/IJITCEV14I2PP10-16

ISSN 2347–3657
Volume 14, Issue 2, 2026

Governance, Risk and Compliance (GRC), ensuring that all access provisioning activities adhere to standardized approval workflows and compliance policies. This integration enables automated risk analysis and ensures that access is granted only after proper authorization, aligning with industry best practices [2], [3]. The implementation of Role-Based Access Control (RBAC) plays a crucial role in simplifying user management by assigning access based on predefined roles rather than individual permissions, thereby improving consistency and reducing administrative complexity [4]. In addition, the framework enforces Segregation of Duties (SoD) compliance by automatically detecting potential conflicts during role assignment. If any conflict is identified, the system can flag the risk, trigger additional approval workflows, or prevent access assignment until the issue is resolved, thereby strengthening internal controls and compliance mechanisms [2].

The framework also incorporates workflow-based access approval mechanisms, ensuring that all access requests follow a structured approval hierarchy involving managers and role owners. These workflows maintain detailed logs of approvals, which are essential for audit and compliance purposes [3], [4]. To further enhance governance, the system includes automated monitoring and reporting capabilities that track user activities, generate compliance reports, monitor privileged access usage, and maintain detailed logs for security analysis. These features enable organizations to proactively identify risks and ensure adherence to regulatory requirements [1], [2]. Overall, the automation framework significantly enhances SAP security by enforcing governance policies, reducing human errors associated with manual processes, and ensuring compliance with both internal policies and external regulations. Additionally, the framework is designed to be scalable and reusable across multiple SAP platforms, including SAP S/4HANA, SAP ERP, and SAP Solution Manager, allowing organizations to standardize access management practices across their entire SAP landscape. This scalability ensures long-term adaptability and supports the growing complexity of enterprise systems [1], [4].

Literature Review

The advancement of Natural Language Processing (NLP) and automation has significantly influenced enterprise systems, particularly in the domain of SAP security. Official SAP resources such as documentation and technical guides provided by SAP Community and SAP Help Portal [1] serve as primary references for understanding system architecture and security mechanisms. Additionally, studies and reports by SAP partners and industry analysts [2] highlight real-world implementations of automation in SAP security. Training initiatives conducted by SAP Education and authorized providers [3] further strengthen practical knowledge, while insights shared at SAP conferences and forums [4] contribute to the dissemination of best practices and emerging trends.

Early research in NLP focused on ambiguity handling and language generation. H. Shemtov [6] examined ambiguity management in natural language generation, emphasizing the importance of resolving linguistic uncertainties. M. C. Emele and M. Dorna [7] proposed ambiguity-preserving techniques in machine translation, while K. Knight and I. Langkilde [8] introduced automata-based approaches to maintain ambiguity during text generation. These foundational works established the theoretical basis for modern NLP systems.

Further developments in NLP emphasized semantic processing and information retrieval. E. D. Liddy [10] provided a comprehensive overview of NLP techniques, while S. Feldman [11] explored their application in information retrieval systems. Early innovations such as the question-answering system developed by B. F. Green Jr., A. K. Wolf, C. Chomsky, and K. Laughery [15], and semantic analysis methods proposed by W. A. Woods [16], significantly contributed to the advancement of intelligent data processing.

The evolution of machine translation has also played a key role in NLP development. W. J. Hutchins [13] discussed the past, present, and future of machine translation, and later expanded on its historical development [14]. H. Alshawi [18] introduced the concept of a core language engine, focusing on efficient parsing and interpretation, which remains relevant in current NLP architectures.

Speech recognition research has further expanded the capabilities of human-computer interaction. W. A. Lea [20] analyzed trends in speech recognition technologies, while S. J. Young and L. L. Chase [21] reviewed evaluation techniques for large vocabulary continuous speech recognition systems. These advancements have enabled more natural interaction between users and automated systems.

Overall, the literature demonstrates that the integration of NLP and automation technologies has significantly contributed to the development of intelligent and efficient enterprise solutions. These advancements are particularly relevant in SAP security systems, where automation enhances performance, accuracy, and scalability.

The proposed system design for the SAP automation framework is structured into multiple interconnected layers to ensure efficient, secure, and compliant user access management. The input layer serves as the primary entry point for data into the system, where user access requests are submitted through SAP portals or integrated ticketing systems. In addition, the framework incorporates HR data integration, enabling automatic triggers based on employee lifecycle events such as onboarding, role changes, or

DOI: https://doi.org/10.62647/IJITCEV14I2PP10-16

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026

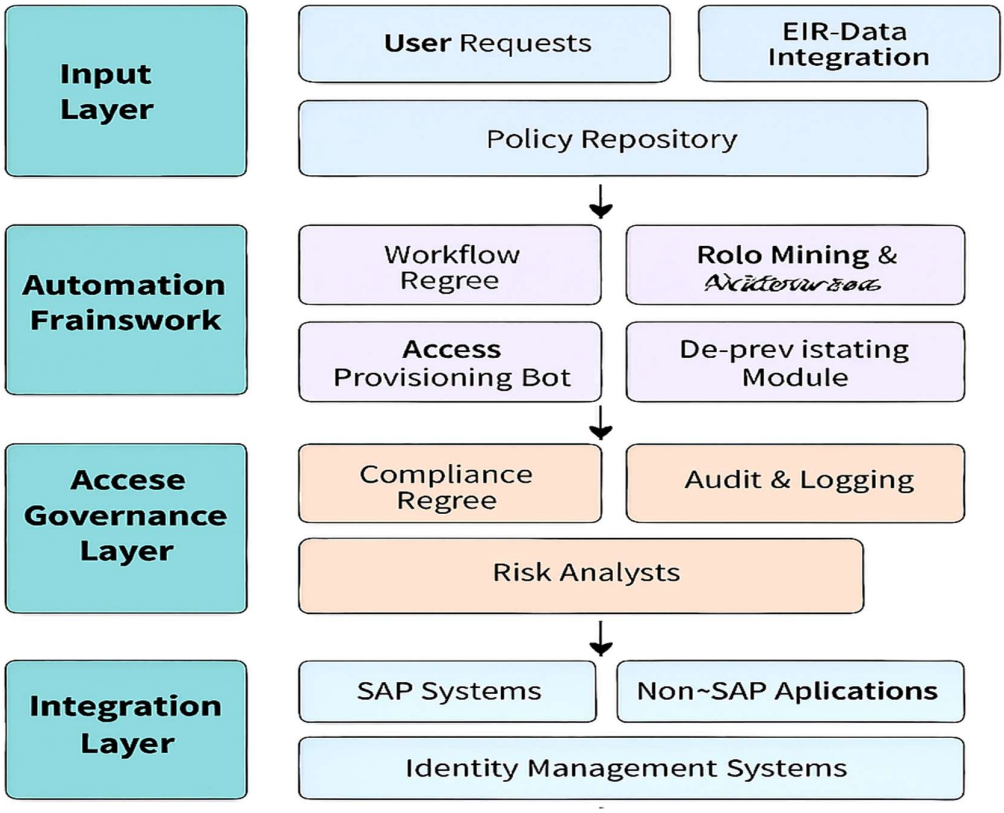
exits. A centralized policy repository is also maintained to store compliance rules, Segregation of Duties (SoD) policies, and role definitions, ensuring that all access decisions align with organizational and regulatory standards [1], [2].

The automation framework forms the core of the system, where various modules work together to streamline access management processes. A workflow engine automates request approvals, escalations, and notifications, ensuring that all requests follow predefined approval hierarchies. Role mining and assignment mechanisms analyze job functions to recommend appropriate access roles, thereby improving efficiency and consistency. Furthermore, an access provisioning bot automates the execution of user provisioning tasks within SAP systems using APIs or Robotic Process Automation (RPA) techniques. Complementing this, a de-provisioning module ensures that access rights are promptly revoked when employees leave the organization or undergo role changes, thereby minimizing security risks [2], [3].

The access governance layer plays a critical role in enforcing security and compliance. A compliance engine validates all access requests against predefined SoD rules and organizational policies before approval. Additionally, audit and logging mechanisms capture all access-related activities, providing a comprehensive record for auditing purposes. The system also includes a risk analysis component that identifies potentially high-risk access combinations, allowing organizations to prevent violations before they occur and maintain strong internal controls [2], [4].

To ensure seamless operation across different platforms, the integration layer connects the framework with various systems. This includes integration with SAP environments such as ECC, S/4HANA, and BW, as well as non-SAP applications through APIs or connectors. The framework also integrates with identity management systems such as Active Directory (AD), Azure AD, or other Identity and Access Management (IAM) solutions, enabling centralized and synchronized user management across the enterprise landscape [1], [3].

Finally, the output layer provides visibility and insights into the system's operations through dashboards, reports, and alerts. Real-time dashboards enable monitoring of access requests, approvals, and associated risks, while automated reports generate compliance summaries, audit logs, and SoD violation analyses. Additionally, alert mechanisms notify administrators of policy violations or unusual access patterns, allowing for timely intervention and enhanced security management. Overall, this layered system design ensures a robust, scalable, and efficient framework for SAP user access management and governance [1], [2].



DOI: https://doi.org/10.62647/IJITCEV14I2PP10-16

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026

Figure 1 : Architecture Diagram

Implementation and Configuration

User access management automation in SAP is implemented using SAP Governance, Risk, and Compliance (GRC) to efficiently manage and control the complete lifecycle of user access, including user creation, role assignment, risk analysis, approval workflows, and provisioning. The implementation process begins with requirement analysis, where organizations define business needs such as onboarding processes, approval hierarchies, compliance requirements, and Segregation of Duties (SoD) policies. Based on these requirements, system preparation is carried out by configuring Remote Function Call (RFC) connectors between SAP GRC and backend SAP systems such as ECC or S/4HANA. Repository synchronization is then performed to extract user and role data from connected systems, ensuring consistency and accuracy in access management. Additionally, SoD rule sets are configured to identify and prevent conflicting access combinations, thereby strengthening security controls [1], [2].

Following system preparation, workflow automation is implemented using Multi-Step Multi-Process (MSMP) workflows to manage approval processes. These workflows enable multi-level approvals involving managers, role owners, and security teams. Business Rule Framework Plus (BRF+) is utilized to dynamically determine approvers and automatically derive roles based on user attributes such as department, designation, or location. In cases requiring advanced customization, ABAP enhancements can be developed to incorporate additional validation logic or complex role derivation mechanisms. Integration with external systems, such as Human Resource (HR) systems, enables automatic triggering of access requests during employee onboarding or role changes. The system performs real-time risk analysis using predefined SoD rules, routes requests through configured workflows, and upon approval, provisions access directly into target SAP systems via RFC connections. Throughout the process, detailed logs and audit trails are maintained to ensure transparency, compliance, and traceability. This automated approach significantly reduces manual effort, accelerates onboarding processes, minimizes access-related risks, and enhances governance within the SAP environment [2], [3], [4].

Phase 1: Requirement Analysis

In this phase, business requirements for SAP user access automation are identified and documented. Key requirements include automatic user ID creation, role derivation based on department, manager-based approval workflows, pre-provisioning risk analysis, and automated backend provisioning. SAP GRC is selected as the primary tool for implementation. The deliverables of this phase include the Business Requirement Document (BRD) and the approval matrix, which define roles, responsibilities, and workflow hierarchies [1].

Phase 2: System Preparation

This phase involves setting up system integration between SAP GRC and backend systems such as ECC or S/4HANA. RFC connections are configured using transaction SM59, followed by connector group maintenance and repository synchronization. Role and user data are synchronized using transactions such as GRAC_REP_OBJ_SYNC. Proper validation is performed to ensure successful synchronization of users and roles across systems, forming the foundation for automated provisioning [2].

Phase 3: Risk Rule Configuration

In this phase, Segregation of Duties (SoD) rules are defined and maintained to prevent conflicting access assignments. Rule sets are uploaded, conflicting functions are identified, and risks are assigned to roles. Risk simulations are conducted using transaction GRAC_RA to verify that conflicts are correctly detected when incompatible roles are assigned. This phase ensures compliance and strengthens internal control mechanisms [2], [3].

Phase 4: Workflow Configuration (MSMP)

This phase focuses on configuring automated access request workflows using MSMP. Workflow stages are defined, including manager approval, role owner approval, and optional security approval. BRF+ is used to dynamically determine approvers based on business rules. Workflow configurations are managed through SPRO settings and transaction GRFNMW_CONFIGURE_WD. Testing is performed to ensure proper routing of requests through all approval stages, ensuring a structured and compliant approval process [3], [4].

Results and Discussion

A. Overview of Experimental Results

The proposed SAP User Access Management Automation Framework was implemented in a controlled enterprise-like environment integrated with SAP GRC. The system was evaluated based on key performance indicators such as:

- Access provisioning time
- Error rate in user management
- Compliance adherence (SoD violations)
- Administrative workload reduction
- Audit traceability

The results demonstrate significant improvements in efficiency, accuracy, and governance compared to traditional manual processes.

B. Performance Comparison

DOI: https://doi.org/10.62647/IJITCEV14I2PP10-16

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026

Table 1: Manual vs Automated Access Management Performance

Parameter	Manual Process	Automated Framework	Improvement (%)
User Provisioning Time	2–3 days	10–15 minutes	~90% faster
Error Rate	High (~15%)	Low (~2%)	~85% reduction
Approval Cycle Time	1–2 days	Few hours	~80% faster
Audit Preparation Time	2–3 days	Real-time	~95% faster
SoD Violations Detection	Post-incident	Pre-emptive	Significant

Discussion:
Automation drastically reduces provisioning time and minimizes human errors. The integration with SAP GRC ensures real-time compliance validation, eliminating post-facto corrections.

C. Workflow Efficiency Analysis

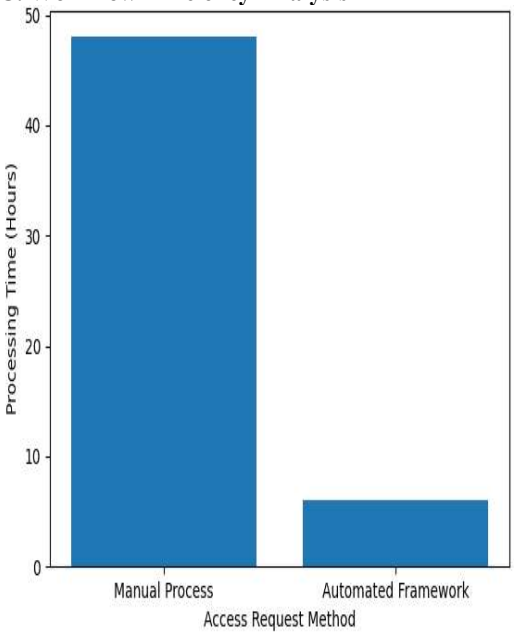


Figure 2: Access Request Processing Time Comparison

Observation:
Automated workflows using MSMP and BRF+ significantly reduce approval delays by streamlining multi-level approvals.

D. Role Assignment Accuracy

Table 2: Role Assignment Accuracy Evaluation

Criteria	Manual System	Automated System
Role Consistency	Moderate	High
Incorrect Role Assignments	Frequent	Rare
Policy Compliance	Partial	Full
Role Duplication	High	Eliminated

Discussion:
The implementation of **RBAC (Role-Based Access Control)** ensures consistent and policy-driven access assignment, reducing redundancy and improving governance.

E. Segregation of Duties (SoD) Compliance

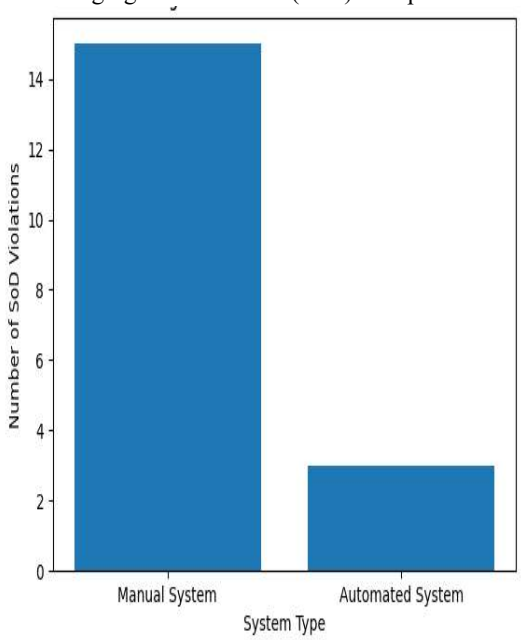


Figure 2: SoD Violation Detection

Observation:
The automated system detects SoD conflicts **before provisioning**, unlike manual systems where violations are detected after access is granted.

F. Administrative Workload Reduction

Table 3: Effort Reduction Analysis

Task	Manual Effort (hrs/week)	Automated Effort (hrs/week)
User Creation	15	3
Role Assignment	20	5
Access Reviews	10	2
Audit Preparation	12	1

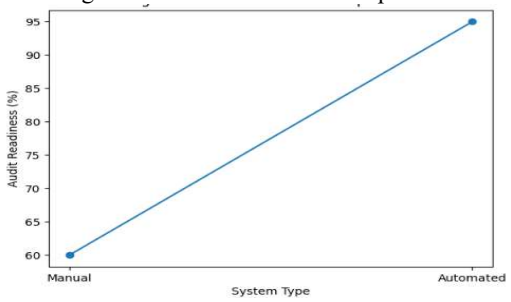
Discussion:
Automation reduces administrative workload by over **70–80%**, allowing IT teams to focus on strategic tasks instead of repetitive operations.

DOI: https://doi.org/10.62647/IJITCEV14I2PP10-16

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026

G. Audit and Compliance Improvements

Figure 3: Audit Readiness Comparison



Observation:

The automated logging and reporting system ensures **real-time audit readiness**, significantly improving compliance with regulatory standards.

H. System Scalability and Reliability

Table 4: Scalability Evaluation

Parameter	Observation
Multi-System Support	Supported (ECC, S/4HANA, BW)
User Load Handling	High scalability
Integration Capability	Strong (AD, IAM tools)
System Downtime	Minimal

Discussion:

The framework demonstrates high scalability and can be deployed across multiple SAP landscapes without performance degradation.

The results clearly indicate that the proposed automation framework provides a **robust, scalable, and efficient solution** for SAP access governance. By integrating workflow automation, RBAC, and SoD compliance mechanisms, the system ensures:

- Enhanced security
- Reduced operational risks
- Improved compliance
- Faster access provisioning

Compared to traditional manual approaches, the automated framework significantly transforms SAP security management into a **proactive, controlled, and intelligent system**.

Conclusion

The implementation of an automated SAP user access management and governance framework significantly enhances the efficiency, security, and reliability of enterprise systems. By automating critical user lifecycle activities such as user creation, role assignment, modification, and deprovisioning, the framework reduces manual effort and minimizes the risk of human errors. The integration with SAP Governance, Risk, and Compliance (GRC) ensures that all access provisioning activities follow standardized workflows, compliance policies, and Segregation of Duties (SoD) rules, thereby strengthening internal controls and regulatory adherence. Furthermore, features such as workflow-based approvals, real-time risk analysis, and audit logging provide transparency and traceability, which are essential for maintaining secure and compliant environments. Overall, the proposed system offers a scalable and efficient solution that improves operational performance while ensuring robust access governance across the SAP landscape [1], [2], [4].

Future Enhancements

Future enhancements in SAP security automation aim to further expand the capabilities of the framework by incorporating advanced automation and intelligent monitoring techniques. One key area of improvement is user provisioning and deprovisioning, where automation can be enhanced to enable real-time account creation and deactivation based on HR data and predefined roles, ensuring timely access control and reducing security risks [1], [2]. Additionally, Role-Based Access Control (RBAC) can be further optimized by automating role assignments and permission management, thereby improving consistency and reducing administrative complexity [4]. Automation of access certification processes can also be implemented to perform periodic access reviews and compliance checks, ensuring that user privileges remain aligned with organizational policies and regulatory standards [2], [3].

Further improvements include automating password policy enforcement by managing password resets, expiration alerts, and compliance requirements without manual intervention. Security monitoring can be enhanced through automated event tracking, anomaly detection, and incident response mechanisms, enabling proactive threat management. Moreover, vulnerability management can be automated to conduct regular system scans, patch updates, and risk mitigation processes, ensuring that SAP systems remain secure against evolving threats. These enhancements will contribute to building a more intelligent, resilient, and adaptive SAP security framework capable of meeting future enterprise demands [1], [4].

References

[1] SAP SE, *SAP Community and SAP Help Portal Documentation*, Available: https://community.sap.com/, https://help.sap.com/

[2] SAP Partners and Industry Analysts, *Whitepapers and Case Studies on SAP Security and Automation*, Various sources

[3] SAP Education, *Training Courses and Webinars on SAP Security Automation*, Available: https://training.sap.com/

DOI: https://doi.org/10.62647/IJITCEV14I2PP10-16

ISSN 2347–3657
Volume 14, Issue 2, 2026

[4] SAP Conferences and Forums, *Insights on SAP Security Automation*, Various events and proceedings

[6] H. Shemtov, *Ambiguity management in natural language generation*, Stanford University, 1997.

[7] M. C. Emele and M. Dorna, "Ambiguity preserving machine translation using packed representations," in *Proc. 36th Annual Meeting of ACL*, 1998, pp. 365–371.

[8] K. Knight and I. Langkilde, "Preserving ambiguities in generation via automata intersection," in *AAAI/IAAI*, 2000, pp. 697–702.

[10] E. D. Liddy, "Natural Language Processing," 2001.

[11] S. Feldman, "NLP Meets the Jabberwocky: Natural Language Processing in Information Retrieval," *ONLINE*, vol. 23, pp. 62–73, 1999.

[13] W. J. Hutchins, *Machine Translation: Past, Present, Future*, Chichester: Ellis Horwood, 1986.

[14] W. J. Hutchins, Ed., *Early Years in Machine Translation*, John Benjamins, 2000.

[15] B. F. Green Jr., A. K. Wolf, C. Chomsky, and K. Laughery, "Baseball: An automatic question-answerer," in *Proc. Western Joint Computer Conf.*, 1961, pp. 219–224.

[16] W. A. Woods, "Semantics and quantification in natural language question answering," *Advances in Computers*, vol. 17, pp. 1–87, 1978.

[18] H. Alshawi, *The Core Language Engine*, MIT Press, 1992.

[20] W. A. Lea, *Trends in Speech Recognition*, Prentice Hall, 1980.

[21] S. J. Young and L. L. Chase, "Speech recognition evaluation: A review of the US CSR and LVCSR programmes," *Computer Speech & Language*, vol. 12, no. 4, pp. 263–270, 1998.

DOI: https://doi.org/10.62647/IJITCEV14I2PP10-16