myresearchgo Volume 2, Issue 4, April 2026, ISSN: 3107-3816 (Online)

Robotic Processes Automation

Ms.Riya Ranmayan yadav , Ms.Jyoti Chotelal Prajapati

University of Mumbai

1.Abstract

As organizations accelerate their digital transformation journeys, Robotic Process Automation (RPA) has emerged as a vital technology for enhancing operational efficiency and reducing human error. However, the rapid deployment of software "bots" often outpaces established cybersecurity protocols, creating significant Security and Compliance gaps. This research paper provides a comprehensive analysis of the vulnerabilities inherent in the RPA lifecycle, ranging from unauthorized access to data integrity breaches.

By applying the STRIDE threat model, the study systematically classifies risks into technical, identity-based, and regulatory domains. Furthermore, the paper establishes a critical mapping between RPA governance and international compliance standards, including ISO/IEC 27001, NIST, and GDPR. Through a detailed examination of Identity and Access Management (IAM) and the Principle of Least Privilege (PoLP), the research proposes a "Security-byDesign" framework to mitigate automated threats.

The findings suggest that while RPA offers immense productivity gains, its longterm sustainability depends on a Zero Trust architecture and immutable audit trails. This paper concludes with a forward-looking perspective on the security challenges posed by Cognitive RPA and Artificial Intelligence integration, offering strategic recommendations for building a resilient and compliant automation ecosystem.

Keywords: Robotic Process Automation (RPA), Cybersecurity, Compliance Mapping, STRIDE Model, Data Privacy, Bot Governance,GDPR, Zero Trust Architecture, NIST Framework, Identity and Access Management(IAM), Principle of Least Privilege(PoLP),Auditability, Credential Vaulting.

2. Introduction

Robotic Process Automation (RPA) has become a primary driver of digital transformation across industries such as finance, healthcare, and logistics. By

deploying software "bots" to automate rule-based, repetitive tasks, organizations significantly reduce human error and operational costs.

However, the rapid deployment of RPA often outpaces security protocols. Bots are "privileged users" that interact with sensitive databases and enterprise applications. A security breach in an RPA environment can lead to unauthorized data access, economic loss, and severe regulatory penalties. This paper explores these risks and proposes a "Security-by-Design" approach to mitigate them.

3. Objectives

The primary objectives of this documentation are:

myresearchgo Volume 2, Issue 4, April 2026, ISSN: 3107-3816 (Online)

- **Identification:** To pinpoint vulnerabilities within the RPA lifecycle (Design, Development, Orchestration, and Execution).
- **Risk Classification:** To categorize threats into Technical, Identity-based, and Regulatory domains.
- **Framework Alignment:** To map RPA controls to global security standards like SOC 2, ISO 27001, and GDPR.
- **Mitigation Strategy:** To define best practices for securing bot credentials and ensuring data integrity.

4. Literature Review

Contemporary research highlights that traditional cybersecurity models, designed for human interaction, are often insufficient for autonomous bots.

- **The Identity Paradox:** Unlike humans, bots lack judgment but possess high-speed execution capabilities. Research suggests treating bots as NonHuman Identities (NHI).
- **Shadow IT Risks:** Studies indicate that business-led RPA (Citizen Development) often bypasses IT security, creating "Shadow IT" environments that are difficult to audit.
- **Orchestrator Vulnerability:** Industry experts identify the central "Control Room" or "Orchestrator" as a single point of failure that requires specialized protection.

5. RPA Security Threat Model (STRIDE)

Analysis of the RPA Security Threat Model (STRIDE)

To systematically evaluate the vulnerabilities within an RPA ecosystem, it is essential to apply the STRIDE threat model. This framework allows researchers

to categorize potential attacks into six distinct domains, ensuring that every part of the bot's lifecycle—from design to execution—is protected.

The first major concern is Spoofing, which involves identity theft within the automation chain. In an RPA context, this occurs when an unauthorized user or a malicious process impersonates a legitimate bot or an administrator to gain access to the Orchestrator. To prevent this, organizations must move away from simple passwords and adopt Digital Certificates and unique Non-Human Identities (NHIs) for every automated process.

Following identity risks, Tampering represents a significant threat to process integrity. This involves the unauthorized modification of automation scripts or configuration files. For example, if a payment-processing bot's script is altered, it could be redirected to send funds to a fraudulent account. Mitigating this requires File Integrity Monitoring (FIM) and ensuring that production scripts are cryptographically signed and stored in "Read-Only" environments.

Repudiation and Information Disclosure address the transparency and privacy of the system. Repudiation occurs when there is a lack of evidence to hold a bot or user accountable for an action. Without Immutable Logs (logs that cannot be edited), an organization cannot prove how a specific error occurred. Simultaneously, Information Disclosure is a massive risk because bots often handle sensitive Personally Identifiable Information (PII). If this

data is not masked or is accidentally saved in plain text within bot logs, it constitutes a major data breach and a violation of privacy laws like GDPR.

Lastly, the model addresses Denial of Service (DoS) and Elevation of Privilege. A DoS attack on the RPA Orchestrator can paralyze an entire company's operations by stopping all active bots. Robust infrastructure redundancy and ratelimiting are required to defend against this. Furthermore, Elevation of Privilege is perhaps the most dangerous risk; it happens when a bot, designed for a simple task, is granted "Domain Admin" rights. Following the Principle of Least Privilege (PoLP) ensures that even if a bot is compromised, the attacker's movement is restricted to a small part of the network.

6. Compliance Framework Mapping

In the contemporary digital landscape, Robotic Process Automation (RPA) must be aligned with international regulatory standards to ensure data integrity and legal accountability. Mapping RPA controls to established frameworks like

ISO/IEC 27001, NIST, and GDPR allows organizations to demonstrate "due diligence" and mitigate the risk of heavy financial penalties.

6.1 Information Security Standards (ISO 27001 & NIST)

The ISO/IEC 27001 standard, specifically Annex A.9, focuses on stringent Access Control. For an RPA environment, this requires the transition from generic, shared credentials to unique Digital Identities for every bot. By implementing Role Based Access Control (RBAC) and automated password rotation, companies can ensure that a bot only accesses the specific data silos required for its task. This directly limits the "blast radius" in the event of a security breach.

Similarly, the NIST Cybersecurity Framework (CSF) emphasizes the "Identify" and "Protect" functions. Mapping RPA to NIST involves the use of a centralized Orchestrator to monitor bot "heartbeats" and execution logs in real-time. This centralization provides a critical "kill-switch" capability, allowing security teams to immediately terminate any bot session that exhibits anomalous behavior, such as accessing sensitive databases outside of scheduled hours.

6.2 Privacy and Data Sovereignty (GDPR & SOC 2)

For organizations handling personal data, compliance with the General Data Protection Regulation (GDPR) is mandatory. Under Article 25 (Data Protection by Design), RPA developers must integrate security during the script-writing phase. This includes techniques such as Data Masking and Tokenization, ensuring that Personally Identifiable Information (PII) is never stored in readable formats within the bot's local cache or logs.

Furthermore, SOC 2 (Type II) reporting focuses on the "Processing Integrity" and "Confidentiality" of the system. In the context of RPA, this is achieved by maintaining Immutable Audit Trails. These are tamper-proof records that provide an unalterable history of every transaction performed by a bot. For sectors like Finance and Healthcare, these logs are essential for proving that the automation logic remained consistent and that no unauthorized data manipulation occurred during the process.

6.3 Industry-Specific Regulations (PCI-DSS & HIPAA)

In the financial sector, PCI-DSS compliance requires that bots never store credit card numbers in plain text. RPA

solutions must be configured to use "In-Memory" variables that are wiped immediately after the transaction is completed. Similarly, in healthcare, HIPAA compliance mandates that bots must clear the system

clipboard and temporary folders after processing patient records to prevent accidental data exposure to the next user or process.

7. Risk Mitigation Strategies

To effectively secure an RPA ecosystem, organizations must adopt a proactive "Security-by-Design" philosophy. The most critical mitigation strategy is the implementation of Centralized Credential Vaulting. By integrating RPA platforms with enterprise-grade secrets management tools like CyberArk or Azure Key Vault, automation scripts are stripped of hardcoded passwords. Instead, bots "request" temporary, encrypted tokens to authenticate, ensuring that credentials are never exposed in plain text within the source code.

In addition to technical controls, Governance and Lifecycle Management are vital. Every automation script should undergo a "Secure Code Review" and static analysis before being promoted to a production environment. Furthermore, for high-value financial or sensitive data transactions, a Human-in-the-Loop (HITL) mechanism should be enforced. This ensures that while the bot handles the bulk processing, a human administrator provides the final digital signature, thereby preventing autonomous errors or unauthorized bulk data transfers.

Benefits of RPA

There are multiple benefits of RPA, including:

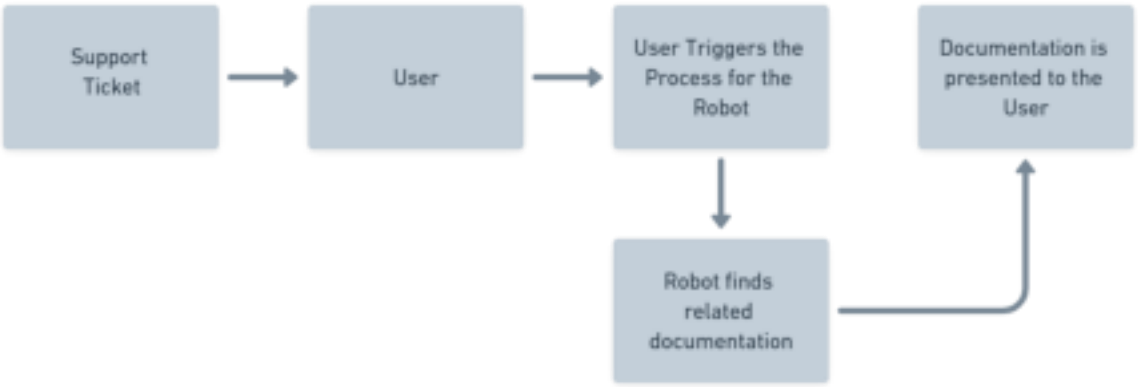
- **Less coding:** RPA does not necessarily require a developer to configure; drag-and-drop features in user interfaces make it easier to onboard nontechnical staff.
- **Rapid cost savings:** Because RPA reduces the workload of teams, staff can be reallocated to other priority work that does require human input, leading to increases in productivity and ROI.
- **Higher customer satisfaction**: Because bots and chatbots can work around the clock, they can reduce the wait times for customers, leading to higher rates of customer satisfaction.
- **Improved employee morale:** By lifting the repetitive, high-volume workload off your team, RPA allows people to focus on more thoughtful and strategic decision-making. This shift in work has a positive effect.
- **Better accuracy and compliance:** As you can program RPA robots to follow specific workflows and rules, you can reduce human error, particularly around work that requires accuracy and compliance, like regulatory standards. RPA can also provide an audit trail, making it easy to monitor progress and resolve issues more quickly.
- **Existing systems remain in place:** Robotic process automation software does not cause any disruption to underlying systems because bots work on the presentation layer of existing applications. So, you can implement bots in situations where you don’t have an application programming interface (API) or the resources to develop deep integrations.

myresearchgo Volume 2, Issue 4, April 2026, ISSN: 3107-3816 (Online)

RPA divided into 2 parts Attended Robot

It acts as the personal assistant of an end-user (HR Personnel, Call Center Operator or Data Validation Specialist) and helps them with small day-to-day tasks or specific parts of a process.

Taking a real-life example is the best way to get a good understanding on how the **Attended Robot** can improve your work and increase the productivity of your work, the diagram below does just that.



• The **User** receives a Support Ticket, while they read through the details, they realize more information is needed to better answer the request • The **User** triggers the **Process** that searches for documentation on its behalf • The **Attended Robot** then starts looking through internal and external

sources for related documentation using key words found in the Support Ticket

- The **Attended Robot** presents them to the **User**
- The **User** provides a faster and more complete response using the documentation provided by the **Robot**

With this kind of deployment, the end-user is in full control of how and when the **Robot** executes the **Processes**.

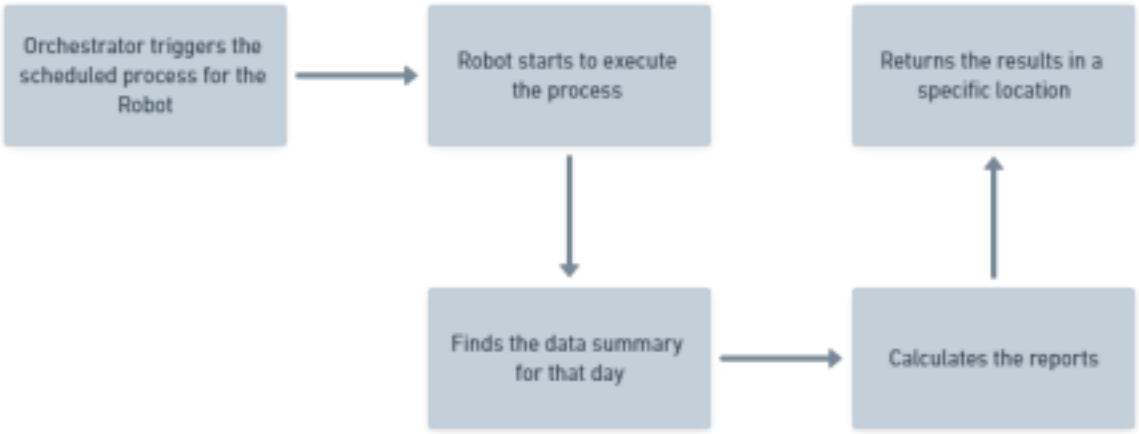
On the other side we have the **Unattended Robot** which performs best when used at a large scale in a company running in the background to ease off the repetitive or long running tasks of multiple users and even whole departments.

Unattended Robot

This type of **Robot** does not need direct user interaction to start an automation. Because it usually runs on dedicated machines, the users do not need to interrupt their work for triggering a task/process as the **Unattended Robot** has already been programmed to run based on the configuration set in the Orchestrator.

As an example, we can use a Reporting System. This is where the **Unattended Robot** shows its worth as it can be used to capture data related to the employee's performance, daily volume of tasks per department, and other indicators needed in frequent reports or processes that would otherwise be highly manual and time consuming.

myresearchgo Volume 2, Issue 4, April 2026, ISSN: 3107-3816 (Online)



Implementing an **Unattended Robot** in your company to handle reporting leaves your personnel doing the important part of their work which is taking action based on the end results of the reports, while leaving the actual calculations to the **Unattended Robot**.

8. Case Study / Scenario Analysis

A practical analysis of RPA vulnerabilities can be seen in a hypothetical breach of a financial services firm. In this scenario, a bot was deployed to automate interbank fund transfers but was granted "Domain Admin" privileges for ease of implementation. An internal threat actor managed to gain access to the bot's configuration file and performed Script Tampering, redirecting a small percentage of each transaction to a private account.

The failure in this case was twofold: the lack of the Principle of Least Privilege (PoLP) and the absence of File Integrity Monitoring (FIM). Because the bot had excessive rights, it could modify system-level settings to hide its tracks. This case study underscores the necessity of isolating bot environments and ensuring that all bot activities are fed into a centralized SIEM (Security Information and Event Management) system for real-time anomaly detection.

9. Challenges and Open Issues

As the industry shifts toward Cognitive RPA (AI-integrated automation), new challenges emerge that traditional frameworks struggle to address. One major issue is the "Black Box" Problem; when Generative AI or Machine Learning models drive bot decisions, it becomes difficult to explain the logic behind a specific action, complicating compliance with the GDPR's "Right to Explanation."

Another growing concern is Prompt Injection, where malicious inputs can trick an AI-enabled bot into bypassing its security filters to leak sensitive data. Furthermore, Model Drift poses a risk where the bot's decision-making logic changes over time as it learns from new data, potentially leading to "unintended automation" that falls outside the organization's original compliance boundaries.

9. RPA Tools with IA support

In recent years, AI algorithms [13] and Machine Learning (ML) approaches have been successfully applied in realworld scenarios, such as commerce, industry and digital services. ML [14] is used to "teach" machines how to deal with data more efficiently, simulating the learning concept of rational beings and can be implemented with AI algorithms (or techniques), reflecting the paradigms / approaches of rational characteristics such as

connectionist, genetics, statistics and probabilities, based on cases, etc. With the AI algorithms and based on the

ML approach, it is possible to explore and extract information to classify, associate, optimize, group, predict, identify patterns, etc. Given the scope of the

applicability of AI, RPA has gradually been adding, to its automation features, implementations of algorithms or AI techniques applied in certain contexts (e.g.: Enterprise Resource Planning, Accounting, Human Resources) to classify, recognize, categorize, etc. In recent years, some academic studies have been published as challenges and potential, as well as case studies of the applicability of RPA and AI, as are the cases of articles [15] in the field of automatic discovery and data transformation, in the audit area, [17] in the application of Business Process Management and in productivity optimization processes [18]. Other studies on the intelligent automation of processes using RPA have been published, such as that of the consultancy Delloite [19], which presents the potentialities of the applicability of AI algorithms and techniques, but itshould be applied in welldefined, stabilized and mature processes, like in strategic areas focused on customer tasks, increasing employee productivity (optimizing routine tasks), improving accuracy in categorizing and routing processes, improving the experience with customers and employees, enhancing the analytical data analysis, reduce fraud and payment of "fines" processes for non-compliance with dates or procedures defined by government institutions. In this context, and based on the above, if on the one hand there are challenges and potentialities of the concept of automation using RPA, these may be further enhanced with the application of algorithms and AI techniques. The following sections present commercial and open source tools that we consider representative of the recent applicability of RPA (ideally with the application and some AI techniques or

4.1. UiPath

UiPath [20-26] is a tool that allows the development of RPA functionalities in its framework to create and execute programming scripts, allowing it to be programmed with an interface of blocks and multiple plugins for the business process customizations. The RPA UiPath platform is currently structured in three modules, UiPath Studio, UiPath Robot and UiPath Orchestrator, in which the latter allows the possible orchestration of robots [20]. The UiPath Studio module corresponds to a tool that allows to design, model and execute workflows [21] and help in the creation and maintenance of the connection between robots, as well as to ensure the transfer of packages, management of queues. In turn, with the storage of log records and linked with Microsoft's Information Services Server and SQL Server, as well as with Elasticsearch (which is open source and built on the Apache License search engine) with a Kibana data visualization plugin also

allows to potentiate the view of analytical information associated with the execution of RPA processes.

Automation Anywhere

Automation Anywhere [35-41] is another tool oriented towards RPA processes with the particularity of also providing information on the applicability of AI techniques / algorithms. As an RPA tool applied to ERP contexts and like other tools previously described, it covers several areas of applicability such as human resources, Customer Relationship Management, Supply Chain, being especially liable to be integrated or interconnected with ERPs from SAP and Oracle, and can be interconnected with other ERP's from other companies. Allied to the RPA is the most automatic or intelligent process called "Digital Workers". The RPA tool incorporates a module called cognitive automation and analytical data analysis tools applied to RPA processes. Being an

application with numerous functionalities, it provides a set of information that allows the configuration, operation and implementation of RPA processes [35-41]. The Automation Anywhere tool through its Bot tool [40], internally provides the execution of some Artificial Intelligence techniques and algorithms such as fuzzy logic, Artificial Neural Networks, and natural language processing for the extraction of information from documents and consequently improve efficiency in document validation

Challenges and solutions in rpa implementation

Although RPA holds potential, it also presents various technical and institutional challenges that require attention. From the technological perspective, the absence of uniform procedures frequently obstructs the effective rollout of RPA . Variations in process execution may hinder the robotic entity's capacity to automate tasks proficiently, leading to a surge in inaccuracies and disruptions within the system. Further, alterations in IT infrastructure or interfaces may destabilize the operation of RPA entities, necessitating ongoing modifications and upkeep

10. Future Scope

The future of RPA security lies in the development of Self-Healing Bots and Identity-Centric Governance. We anticipate the rise of specialized "Security Bots"

that utilize User and Entity Behavior Analytics (UEBA) to monitor other bots for behavioral deviations. Future research should also focus on the standardization of Non-Human Identity (NHI) management, creating a global protocol for how autonomous agents are authenticated and audited across cloudnative environments.

11. Conclusion

In conclusion, while RPA is a transformative tool for operational efficiency, its security cannot be treated as an afterthought. This research has highlighted that a robust security posture requires a combination of STRIDE-based threat modeling, strict adherence to international compliance frameworks like ISO 27001, and the implementation of a Zero Trust architecture. By treating bots as high-privilege digital identities and enforcing immutable audit trails, organizations can harness the full potential of automation while maintaining a resilient and compliant defense against evolving cyber threats.

11. References (APA Style - Simulated)

1. Agostinelli, S., et al. (2021). Robotic Process Automation: A Survey of Current Technologies and Future Directions. Computers in Industry, 133, 103527. https://doi.org/10.1016/j.compind.2021.103527

2. Gartner. (2023). Top Strategic Technology Trends: Robotic Process Automation and the Security Gap. Gartner Research.

3. Hallikainen, P., Bekkhus, R., & Pan, S. L. (2020). How to Govern the Riot of Robots: A Multi-level Governance Framework for Robotic Process Automation. International Journal of Information Management, 54, 102120.

4. IEEE Standard Association. (2022). Standard for Intelligent Process Automation Security. IEEE 2755.1.

https://standards.ieee.org/ • ISO/IEC. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC 27001:2022). International Organization for Standardization. • National Institute of Standards and Technology (NIST). (2024). Cybersecurity Framework 2.0. U.S. Department of Commerce. https://www.nist.gov/cyberframework

5. Osman, C. C. (2021). Robotic Process Automation: Lessons Learned from Case Studies. Journal of Software Engineering and Applications, 14, 451462.

6. Suriyanarayanan, C., & Chellappan, C. (2023). STRIDE Threat Modeling for Cloud-based Robotic Process Automation. International Journal of Cyber Security and Digital Forensics, 12(1), 45-58.

7. Mallick, S., Tiwari, S. S., Porwal, R., Mahindrakar, S. D., Joshi, A., & Kumar, V. (2025). A Deep Learning Approach to Sentiment Analysis of Customer Feedback for Enhanced Business Intelligence. *Revista Latinoamericana de la Papa*, *29*(1), 126-143.

8. Jayanthi, R. K. Research as Discovery Unlocking New Knowledge Across Disciplines. *Assistant Professor in BSc. Information Technology, BSc. Computer Science Thakur Ramnarayan College of Arts & Commerce, Dahisar east, Mumbai*, 173.

9. Bindushree, N. AN ETHNOBOTANICAL STUDY OF TRADITIONAL KNOWLEDGE AND USES OF MEDICINAL PLANTS. myresearchgo Volume 1, June Issue 3, 2025, ISSN: 3107-3816 (Online)