



**National Centre  
of Excellence**

CYBERSECURITY TECHNOLOGY  
AND ENTREPRENEURSHIP



इलेक्ट्रॉनिक्स एवं  
सूचना प्रौद्योगिकी मंत्रालय  
MINISTRY OF  
ELECTRONICS AND  
INFORMATION TECHNOLOGY

**DSCI**  
PROMOTING DATA PROTECTION  
A **nasscom** Initiative

# ROBOTIC PROCESS AUTOMATION (RPA)

## Security Challenges and Future Trends



## **Contributors**

### **Sonam Lata**

Assistant Professor  
Department of Computer Science and Engineering,  
IILM University Gurugram, Haryana India

### **Shabana Mehfuz**

Professor  
Department of Electrical Engineering  
Jamia Millia Islamia

# Table of **CONTENTS**

|  |    |
|--|----|
| Context                                      | 5  |
| 1. Introduction to RPA Security              | 6  |
| 2. The Different Types of Process Automation | 8  |
| 3. Existing Security Tools/Features in RPA   | 11 |
| 4. Challenges in RPA Security                | 14 |
| 5. RPA Security Best Practices Checklist     | 18 |
| 6. Future of RPA Security                    | 21 |
| 7. Conclusion                                | 22 |
| 8. References                                | 23 |





# Context

The focus on RPA security is growing as more businesses adopt robotic process automation (RPA), a technology that uses “bots” to automate repetitive, daily tasks. Because RPA bots can move private information between systems, they can contribute to security lapses like fraud and data leaks if they are not implemented adequately. This shouldn’t stop you from automating your company’s procedures or reaping the rewards of quicker, error-free operations. This guide describes typical obstacles that arise when implementing RPA and how to address security issues to guarantee a secure adoption process. RPA technology, when used correctly, removes manual errors that expose the entire business to data breaches and non-compliance problems. All automated processes, however, are vulnerable to external threats, internal malevolent actors, and other types of malware if proper oversight is not in place. Because RPA can simulate human-computer interactions, security issues arise when unsupervised RPA bots access, edit, or transfer files containing sensitive customer or business data.

# 1

## Introduction to RPA Security

By automating rule-based tasks, robotic process automation, or RPA, has become increasingly popular across industries, helping businesses streamline operations. Notwithstanding its benefits, implementing RPA carries security risks that could result in operational disruptions, data breaches, and noncompliance with regulations. Unauthorized access, data exposure, insider threats, and cyberattacks are major issues with RPA security. A high-level overview of security concerns, legislative and regulatory developments, and industry best practices pertaining to the security of robotic process automation (RPA) is given in this document. This note highlights important factors for policy interventions, but it does not provide concrete solutions for protecting RPA systems. Future studies and technical developments targeted at enhancing the security and compliance of RPA implementations may be guided by the concepts covered in the last section.

By automating repetitive tasks, increasing productivity, and lowering human error, robotic process automation, or RPA, is completely changing how businesses operate. However, as more businesses use RPA solutions, security threats surface that need to be resolved to guarantee system integrity, data protection, and regulatory compliance. In addition to offering best practices to reduce risks and guarantee a safe RPA ecosystem, this white paper examines the foundational elements of RPA security, current security tools, obstacles, and emerging trends in RPA system security.

The focus on RPA security is growing as more businesses adopt robotic process automation (RPA), a technology that uses bots to automate routine, repetitive tasks. Because RPA bots can move private information between systems, they can lead to security lapses like fraud and data leaks if they are not implemented properly. Concerns





regarding data security, regulatory compliance, and operational integrity have been brought up by the broad use of RPA<sup>[1]</sup>.

Businesses shouldn't let this stop them from automating their operations or reaping the rewards of quicker, error-free operations. This white paper describes typical obstacles to RPA deployment and offers advice on addressing security issues to guarantee a secure and efficient automation strategy.

This section examines:

- **How crucial RPA security** is to safeguarding private information and preserving system dependability.
- **Typical security** issues that businesses run into when deploying RPA solutions.
- **Important security threats**, such as privilege escalation, API vulnerabilities, and bot credential theft.
- **Current threat mitigation** techniques and security measures, such as encryption, multi-factor authentication, and role-based access controls (RBAC)<sup>[2]</sup>.

# 2

## Different Types of Process Automation

These days, RPA tools can interact with user interfaces, run scripts, and have specialized tooling to automate intricate business processes. However, RPA tools are much more than just those fundamental features. On a very broad scale, automation falls into four categories, Front-End Automation, Automation of user interfaces, back-end systems, APIs, and native actions, specialized operations aimed at particular business uses, Intelligent Automation for Artificial intelligence and machine learning for situations requiring greater critical thinking

Users can automate a wide range of tasks by combining these four types of automation. Additionally, it incorporates human decision-making logic into the process by incorporating intelligent automation.

### 2.1 Front-End Automation

The methods for simulating human interactions with user interfaces, like those of Windows apps and web browsers, are provided by UI automation. Generally speaking, there are three types of UI automation capabilities:

- a. Windows and legacy applications
- b. Applications for browsers
- c. RDP-based remote desktop programs, among others





Most of the time, the underlying controls interact with the Windows and browser-based capabilities. For instance, when a button is clicked automatically, a “button click” event is triggered on the button. However, the remote session cannot access the underlying application controls when interacting with a remote desktop. Therefore, the RPA application must be able to identify graphical regions that represent the button in order to simulate a button click on a remote desktop.

## **2.2 UI Automation**

Pros of UI Automation includes its ease to use. Since UI automation mimics human steps to complete a task, even non-technical users can automate their work. Sometimes it is the only option for some applications. Some applications only provide a UI for interaction (e.g., browser-based applications). UI automation may be the only option for legacy Windows applications.

Cons of UI Automation are so many. UI Changes May Break Automations Frequent UI updates (e.g., design changes or added features) may disrupt automation. Adjusting the window size may alter the UI layout, affecting automation. Decision-Making is Not Automated. Many UI actions depend on human decision-making, which is not inherently captured. Users need to manually extend the automation to include business logic. UI automation requires control over the mouse and keyboard, preventing simultaneous computer use.

Modern RPA Recorders are of various types such as Macro Recorders. They capture and replay user actions in exact sequence and are quick to implement but cannot be edited or updated. Step Recorders allows users to record and modify each action. Enable debugging and adding business logic.

## **2.2 Back-End Automation: API Automation**

API automation interacts with application programming interfaces (APIs) to accomplish tasks. Example: Automating the transfer of loan applications from an origination service to a processing service. APIs generally follow web services (older) or HTTP-based RESTful standards. Data exchange formats include XML and JSON.

Pros of API Automation are Robustness. APIs rarely change and often support older versions. Not impacted by desktop changes (e.g., window resizing). Background Execution: API automations run without interfering with desktop activities.

Technical Knowledge Required: Users must understand APIs and data formats, making it less accessible to non-technical users.

Native Actions provides user-friendly automation for specific applications (e.g., FTP, Microsoft apps, databases). Unlike UI or API automation, native actions are built for a single application.

Widely Used Applications are Email, Microsoft Office. Applications without UI or Standard API (e.g., Databases that require direct queries).

Pros of Native Actions are its ease to Use: Custom-built for specific applications, more stable than UI automation. Background Execution: Runs without interfering with desktop work.

Cons of Native Actions are its Limited Availability: Cannot be applied to all applications.

## **2.3 Intelligent Automation**

Intelligent Automation uses AI and Machine Learning (ML) to improve decision-making in automation. Unlike native actions, it is designed for specific capabilities, not specific applications.

AI and ML in Automation helps in decision-making tasks. Modern automation tools integrate with AI/ML frameworks (e.g., TensorFlow, ML.NET). AI capabilities are often provided by specialized companies, rather than being built into RPA tools.

Attended Automation requires human intervention at some stage (e.g., clicking buttons, filling forms, reviewing data). Unattended Automation runs completely without human involvement.

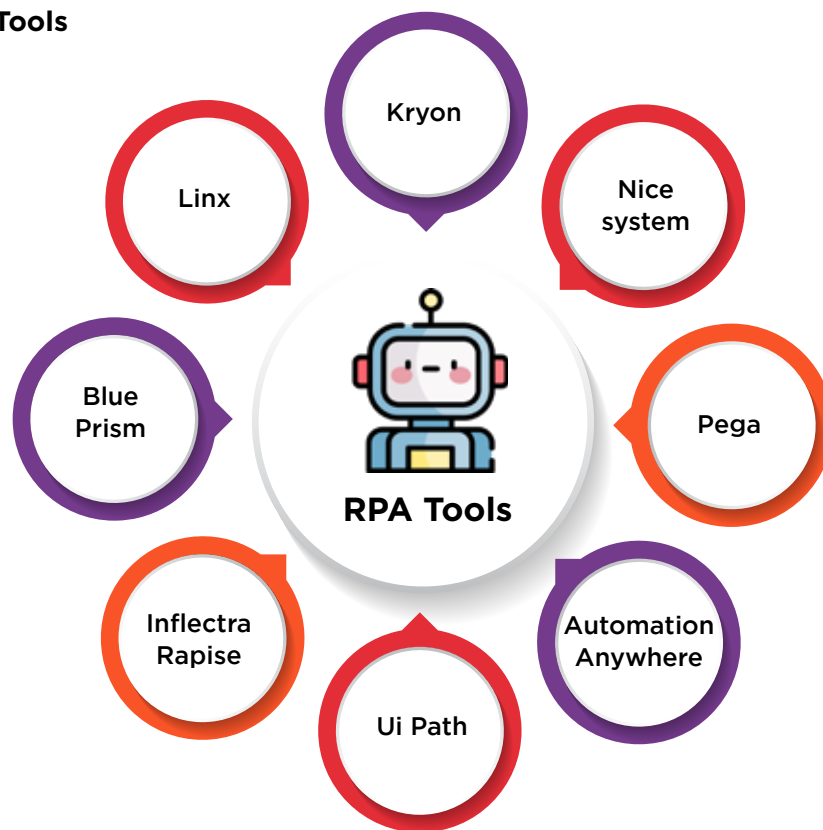
# 3

## Existing Security Tools/Features in RPA

RPA vendors and businesses incorporate a variety of security measures into their platforms to mitigate security threats. Among the crucial security features and tools are:

- **Security Frameworks for RPA Platforms:** Putting security guidelines and standards like GDPR compliance, ISO 27001, and the NIST Cybersecurity Framework into practice <sup>[3]</sup>.
- **Access Control and Identity Management:** To guarantee that only authorized individuals can operate bots, stringent authentication procedures, role-based access control (RBAC), and privileged access management (PAM) are enforced.
- **Data protection and encryption:** putting strong encryption procedures in place to protect data while it's in transit and at rest while lowering the possibility of data breaches.
- **Threat Detection and Prevention:** To detect and lessen possible cyberthreats, AI-driven security analytics, behavior monitoring, and anomaly detection are used.
- **Audit and Compliance Monitoring:** Making certain that every bot interaction is recorded, tracked, and examined for adherence to industry rules<sup>[4]</sup>.

**Figure 1: RPA Tools**



As seen in Figure 1, robotic process automation (RPA) tools assist in automating routine business procedures, which lowers manual labor and boosts productivity. Numerous top RPA tools are shown in the image, each with special features and applications. An explanation of these tools' features and industrial applications is provided below.

#### **a. The Blue Prism**

An established RPA tool with enterprise-grade automation features is Blue Prism. It facilitates safe, scalable automation and offers a low-code interface. The banking, finance, and healthcare industries make extensive use of Blue Prism to automate intricate processes. Key features include cloud and on-premises deployment, centralized control for improved security, and a drag-and-drop automation interface.

#### **b. Rapise Inflectra**

An RPA and test automation tool for desktop, mobile, and web applications is called Inflectra Rapise. It is well-liked for agile software testing and automation, and it is perfect for companies that need testing automation that is flexible. Supporting cross-browser and cross-platform automation, integrating with test management tools such as SpiraTest, and requiring no programming for simple automation tasks are some of its key features.

#### **c. UiPath**

One of the top RPA platforms, UiPath is renowned for its robust automation features and easy-to-use interface. It offers AI-powered automation features and supports both attended and unattended automation. Cloud-based automation and orchestration, drag-and-drop workflow automation, and AI and ML integration for intelligent automation are some of the key features.





#### **d. Automation Anywhere**

An RPA tool called Automation Anywhere provides cloud-native, artificial intelligence (AI)-powered automation solutions. It is extensively utilized in sectors such as manufacturing, healthcare, and BFSI (Banking, Financial Services, and Insurance). Key features include cloud and on-premises RPA deployment, AI-powered task automation with IQ Bot, and the Bot Store for pre-built automation components.

#### **e. Pega**

Pega is a platform for low-code automation that blends business process management (BPM) and RPA. The banking, insurance, and customer service sectors all make extensive use of it. Key features include event-driven automation for customer interactions, AI-powered decision-making for workflow automation, and integrated CRM integration for automated customer engagement.

#### **f. Nice System**

Nice System specializes in customer service automation and offers AI-powered RPA solutions. Through the automation of front-office and back-office tasks, it helps businesses increase efficiency. Key features include AI-powered analytics for process optimization, voice, chat, and document processing automation, and attended automation for contact centers.

#### **g. Kryon**

One RPA tool that is well-known for its automation and process discovery features is Kryon. It assists companies in finding opportunities for automation and streamlining processes. Hybrid RPA (attended and unattended automation), Process Discovery AI for automation recommendations, and smooth integration with business systems are some of the key features.

#### **h. Linx**

For backend automation, API integrations, and workflow automation, Linx is a low-code automation platform. Developers primarily use it to create unique automation solutions. Drag-and-drop backend automation, database and API integration, and multi-programming language support are some of its primary features.

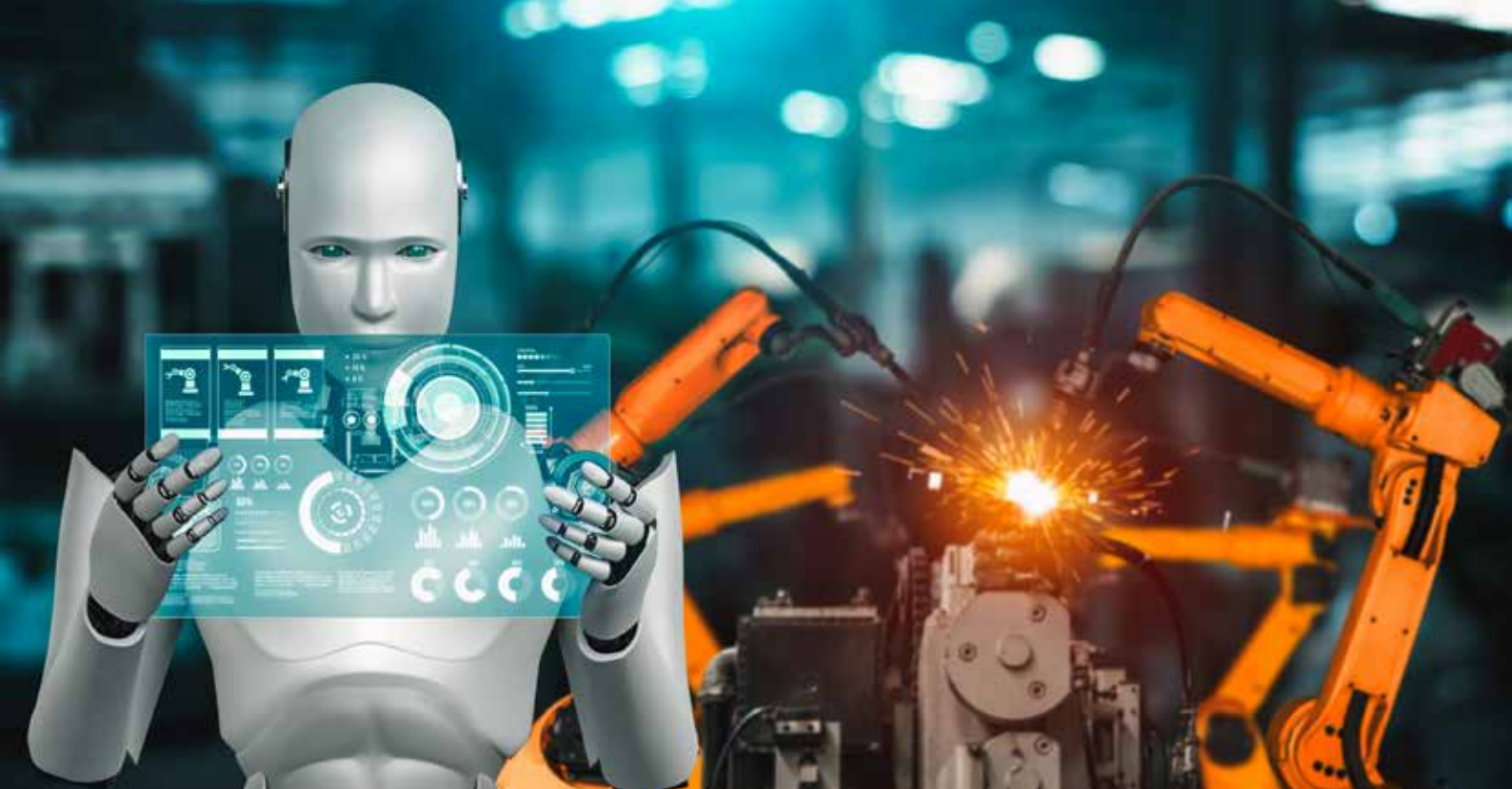
# 4

## Challenges in RPA Security

RPA has an impact on the organization's governance, control, and risk management. First, in order to handle the organizational changes brought about by RPA, organizations' governance strategies will either need to directly integrate RPA into their current governance frameworks or develop new, decentralized governance structures tailored to RPA [5]. Either way, before implementing RPA, governance frameworks should be established [6]. Second, the impact of RPA must be taken into account in risk management plans [7]. RPA software may not properly automate processes and process constraints, which could result in inaccurate process outcomes and unanticipated, risky process exceptions [8]. The risk environment is also impacted by privacy and security issues. Sensitive information may be revealed when collecting digital evidence for an audit [9]. Stated differently, there might be a higher chance of cybersecurity breaches within organizations.

These risk areas may necessitate changes to auditing standards and adjustments to the organization's risk register [10]. The control environment will also need to change as a result of changes in risk and governance. To address the security risks posed by RPA, controls that are designed to reduce those risks must be put in place. Controls that guarantee the confidentiality, integrity, accessibility, accountability, authenticity, and dependability of the data used by the RPA software should be put in place by the organization [11]. Controls that address the potential for flawed RPA workflow should also be in place [12]. In order to assess the effectiveness and sufficiency of these new controls, an audit of the RPA system itself will also be necessary.





The use of RPA by fraudsters presents another challenge when it comes to audit and fraud control. Users may misuse robotic process automation to make fraud easier [13]. Further research is still required to fully understand the connection between RPA and fraud [13].

However, it was discovered that using RPA when providing authorities with information that is considered a banking secret reduced the risk of non-compliance in areas like information protection and fulfilling legal requirements [11]. Therefore, by lowering errors in crucial processes, robotic process automation may also offer a way to address some compliance threats.

To guarantee that strategic objectives are fulfilled, organizations must take into account the different uses of RPA as well as the implications for the environment of risk, control, and organizational governance.

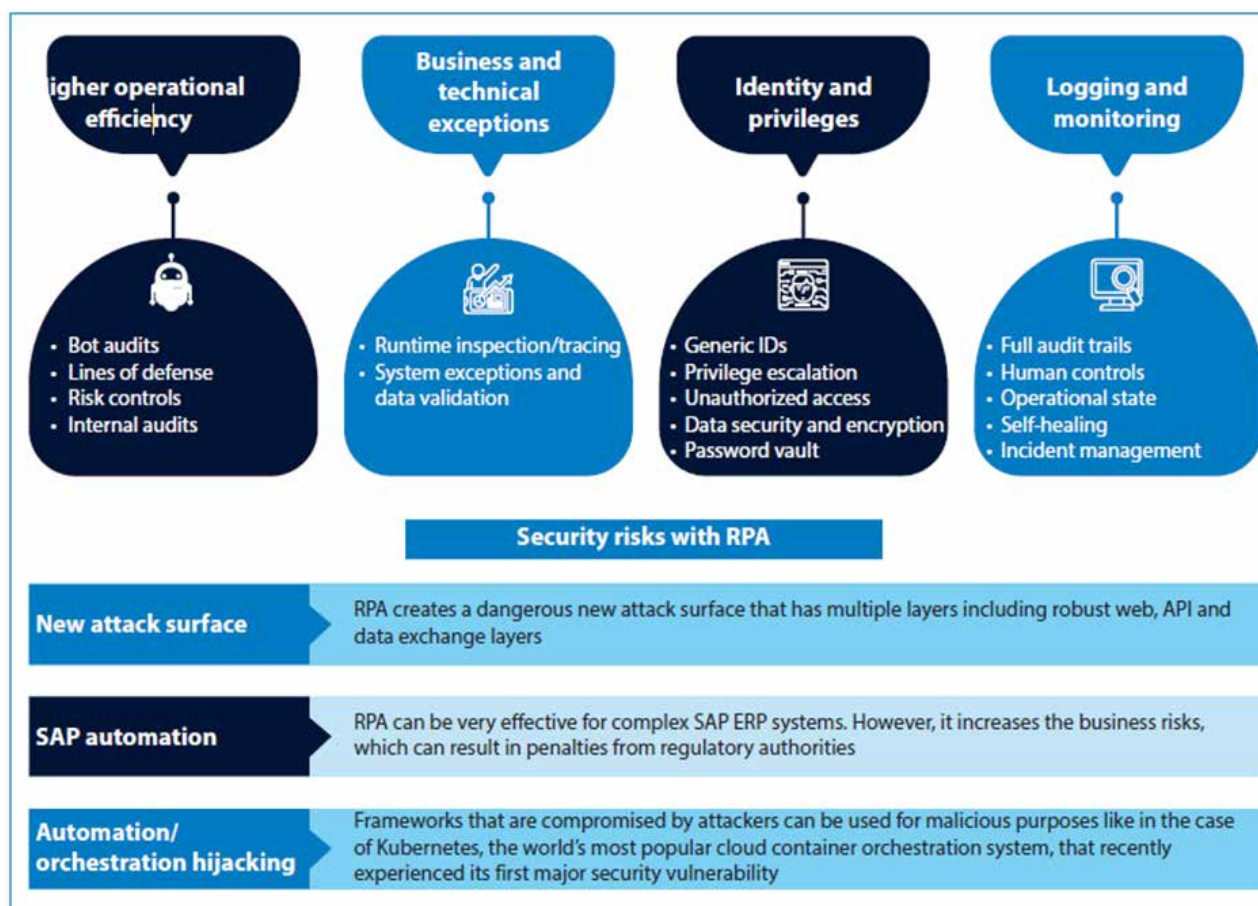
The following eight typical obstacles to a secure RPA approach are depicted in figure 2:

#### **4.1. Accidental data exposure**

RPA bots frequently manage private data, including financial records, customer information, and confidential company information. If RPA bots are not properly configured or left unsupervised, your data could be intercepted by hackers who want to steal or destroy important information.

An RPA bot accidentally sending sensitive data to the incorrect location could be an example of unintentional data exposure. This could expose the business to additional privacy violations and penalties if customer data and other types of personally identifiable information (PII) are made available to unauthorized users.

Figure 2: Security Risks with RPA



## 4.2. Bot impersonation

The idea of assigning a distinct identity to every bot is essential for security and avoiding bot impersonation. When an unauthorized entity poses as a genuine bot to perform actions that might result in illegal activity or security breaches, this is known as bot impersonation.

It can be challenging to identify which bot initiated a particular action when two bots share the same identity. Unauthorized access or potentially dangerous behaviors that are hard to monitor are made possible by this lack of accountability.

## 4.3. Credential storage and management

In order to interact with other platforms, bots need login credentials. Because any flaw in this process could allow for unauthorized access and data manipulation, the way these credentials are stored, retrieved, and handled presents a security risk.

An RPA system is vulnerable to credential theft if it uses shoddy encryption techniques or saves login information in plain text. These flaws could be used by malicious parties to access systems or private data without authorization.

#### **4.4. Oversights in rapid deployment**

The haste with which RPA must be implemented may cause crucial security measures to be overlooked. Unencrypted communication between the RPA bot and backend systems may result from a company's hurried implementation of an RPA solution to automate a manual process without first conducting a comprehensive security assessment. This is a preventable mistake that leaves your RPA strategy open to hacker or other threat interception.

#### **4.5. Dependency on third-party integrations**

RPA systems frequently integrate with other third-party applications and systems. Relying on these integrations introduces additional risks if they are not sufficiently secured.

Suppose an RPA bot uses an unauthorized external program to transfer data; if the external party is compromised or has security flaws, the workflow may be disrupted or the data may be changed.

# 5

## RPA Security Best Practices Checklist

Security in RPA implementation remains a significant challenge. Some key challenges include:

- a. Unintentional Data Exposure: RPA bots manage private data, including financial records, customer information, and confidential company information. They may unintentionally reveal important information to unauthorized users if improperly configured, which could result in compliance violations (Cybersecurity & Infrastructure Security Agency, <sup>[14]</sup>).
- b. Bot Impersonation: Illegitimate entities may pose as trustworthy bots in order to commit fraud or compromise security.
- c. Storage and Management of Credentials: Inadequate credential management raises the possibility of unwanted system access.
- d. Oversight of Rapid Deployment: Companies in a hurry to implement RPA solutions might forget important security precautions, leaving systems exposed.
- e. Third-Party Integrations: RPA systems frequently depend on outside apps, which may result in extra security flaws (Williams & Green, <sup>[15]</sup>).

This checklist shown in figure 3 can serve as a guide for safeguarding automated processes and mitigating potential risks associated with RPA implementation:





## 5.1. Deploy authentication protocols

Give every RPA bot a unique identifier to make sure they can be identified and have particular access rights. This stops illegal use and bot impersonation. As an additional security measure, configure multi-factor authentication (MFA) or other “human-to-system” verification methods.

Figure 3: RPA Security Checklist



## 5.2. Centralize credential management

To manage and monitor all bot credentials in one location, a business can use an encrypted password management system. This guarantees that only authorized individuals can access and update these credentials. The likelihood of unauthorized individuals obtaining sensitive login credentials is reduced as a result of the restricted access.

### **5.3. Implement distinct credentials for each bot**

Assigning distinct login credentials to every bot improves security and accountability. This eliminates the potential for bot impersonation and links each bot's actions to its unique identity.

### **5.4. Proactively monitor bots**

An RPA system can alert administrators if a bot unexpectedly starts gaining access to unapproved systems or departs from its standard operating procedures with the use of monitoring tools. Investigating and resolving potential security issues promptly is made possible by proactive monitoring.

### **5.5. Routinely check RPA scripts**

To make sure RPA scripts adhere to security standards, set up and implement frequent audits. This proactive approach promptly identifies any vulnerabilities or unforeseen risks in the automation scripts and ensures their long-term security and functionality.

### **5.6. Control user access**

Strict access controls should be put in place to restrict access to sensitive information and ensure that only those with the appropriate authorization can view or change important data. Access privileges can be routinely reviewed to ensure that only necessary users handle sensitive data once an RPA system has been set up to restrict access to critical financial data for a specific user group within the organization.

### **5.7. Maintain log integrity**

Protect log files from alteration or unwanted access to maintain log integrity and keep them as trustworthy documentation for audits and investigations. Use access controls to limit who can read, edit, or remove log entries, and encrypt RPA logs to safeguard important company information.



# 6

## Future of RPA Security

Security tactics need to change as RPA adoption keeps increasing in order to handle new threats. The following are some future trends in RPA security:

- **AI-Powered Security Solutions:** Using AI and ML to detect threats, analyze behavior, and identify anomalies in real time.
- **Blockchain for Secure Transactions:** Blockchain technology ensures data integrity and transparency by offering immutable transaction logs.
- **Zero-Trust Security Models:** To reduce the possibility of unwanted access, implement zero-trust architecture.
- **Threat Intelligence Advancements:** To anticipate and stop cyberattacks before they happen, security vendors are creating proactive threat intelligence solutions (Kumar et al., [16]).

# 7

## Conclusion

Ensuring regulatory compliance, safeguarding sensitive data, and preserving data integrity all depend on secure RPA implementations. Businesses need to implement best practices, adopt strong security measures, and keep up with changing threats. Businesses can establish a safe and robust RPA environment that minimizes risks and optimizes automation benefits by utilizing blockchain technology, AI-driven security solutions, and proactive monitoring.

# References

- [1] Smith, J., Roberts, K., & Johnson, M. (2021). Security Risks in RPA: Mitigation Strategies. *Journal of Cybersecurity Research*.
- [2] Brown, L., & Taylor, R. (2022). Automation and Cybersecurity: Managing RPA Threats. *Cybersecurity Trends*.
- [3] National Institute of Standards and Technology. (2021). NIST Cybersecurity Framework. Retrieved from [www.nist.gov](http://www.nist.gov).
- [4] Jones, P., & Patel, D. (2023). Regulatory Compliance in RPA Security. *Compliance Today Journal*.
- [5] Kokina, J., Blanchette, S.: Early evidence of digital labor in accounting: Innovation with Robotic Process Automation. *Int. J. Account. Inf. Syst.* 35, 100431 (2019)
- [6] Steinhoff, J., Lewis, A., Everson, K.: The march of the robots. *J. Gov. Financ.Manage.* 67(1), 26–33 (2019)
- [7] Tucker, I.: Are you ready for your robots? *Strategic Finance* 99(5), 48–53 (2017)
- [8] Syed, R., et al.: Robotic Process Automation: contemporary themes and challenges. *Comput.Ind.* 115, 103162 (2020)
- [9] Moffitt, K.C., Rozario, A.M., Vasarhelyi, M.A.: Robotic process automation for auditing. *J. Emerg. Technol. Account.* 15(1), 1–10 (2018)
- [10] Appelbaum, D., Nehmer, R.: The coming disruption of drones, robots, and bots: how will it affect CPAs and accounting practice. *CPA J.* 87(6), 40–44 (2017)
- [11] Wojciechowska-Filipek, S.: Automation of the process of handling enquiries concerning information constituting a bank secret. *Banks Bank Syst.* 14(3), 175–186 (2019)
- [12] Kaya, C.T., Turkyilmaz, M., Birol, B.: RPA Teknolojilerinin Muhasebe Sistemleri Üzerindeki Etkisi. *Muhasebe ve Finansman Dergisi* 82, 235–250 (2019)
- [13] Nickerson, M.A.: Fraud in a world of advanced technologies: the possibilities are (unfortunately) endless: certified public accountant. *CPA J.* 89(6), 28–34 (2019)
- [14] Cybersecurity & Infrastructure Security Agency. (2022). Guidelines on RPA Security. Retrieved from [www.cisa.gov](http://www.cisa.gov).
- [15] Williams, S., & Green, T. (2022). Risk Assessment in Automated Systems. *Information Security Review*.
- [16] Kumar, R., Lee, H., & Martin, P. (2023). Future Trends in RPA Security. *AI & Cybersecurity Journal*.



The National Centre of Excellence (NCoE) for Cybersecurity Technology Development has been conceptualized by the Ministry of Electronics & Information Technology (MeitY), Government of India, in collaboration with the Data Security Council of India (DSCI). Its primary objective is to catalyze and accelerate cybersecurity technology development and entrepreneurship within the country. NCoE plays a crucial role in scaling and advancing the cybersecurity ecosystem, with a focus on critical and emerging areas of security.

Equipped with state-of-the-art facilities, including advanced lab infrastructure and test beds, NCoE enables research, technology development, and solution validation for adoption across government and industrial sectors. By adopting a concerted strategy, NCoE aims to translate innovations and research into market-ready, deployable solutions—contributing to the evolution of an integrated technology stack comprising cutting-edge, homegrown security products and solutions.




Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by nasscom, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI brings together governments and their agencies, industry sectors including ITBPM, BFSI, telecom, industry associations, data protection authorities and think-tanks for policy advocacy, thought leadership, capacity building and outreach initiatives. For more info, please visit [www.dsci.in](http://www.dsci.in)

## DATA SECURITY COUNCIL OF INDIA

 +91-120-4990253 | [ncoe@dsci.in](mailto:ncoe@dsci.in)

 <https://www.n-coe.in/>

 4 Floor, NASSCOM Campus, Plot No. 7-10, Sector 126, Noida, UP -201303

### Follow us on

 @CoeNational

 nationalcoe

 nationalcoe

 NationalCoE