IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AI And ML-Based RPA For Automated Incident Management In Cybersecurity

Abhaykumar Dalsaniya

Independent Researcher, Principal Architect

Abstract

Cybersecurity risks have promulgated the researcher's argument for efficient and effective models for managing incidents. Most traditional methods of executing tasks entail using human resources, which results in slow performance and costly errors. Understanding the new role of AI and ML applications in RPA for optimizing the progressive execution of automated incident management in contextualizations of cybersecurity is crucial for this paper. With the integration of AI and ML, the RPA can analyze large volumes of data and find inconsistent patterns and probable threats quickly; hence, better responses can be made. This paper also reviews different AI and ML approaches that might be applied to ensure efficient threat identification, pattern recognition, and incident resolution. Only practical examples are presented to illustrate the algorithms' effectiveness.

Further, the paper presents primary issues and alternatives that cover technical issues and ethical concerns regarding the employment of AI-activated automation. As highlighted in the study, adopting RPA by incorporating AI and ML enhances service delivery and minimizes the time and resources needed to manage the incidents. Therefore, it is a rich source of knowledge enhancement for modern cybersecurity mechanisms.

Keywords: RPA, Cyber threat, IBM security, Cyber security

1. Introduction

1.1 Background to the Study

The threats are more pronounced, especially in the current generation, with threats arising more frequently and being very complex (Verizon, 2021). As attacks via advanced persistent threats (APTs), ransomware, and other zero-day threats continue to rise, conventional security approaches have been rendered inadequate, fuelling the drive to enhance modern incident management ENISA, 2020 systems. These threats jeopardize data and hinder essential processes, which is costly and damaging to reputations (IBM Security, 2020).

Certainly, conventional methods of managing incidents involve extensive paperwork – and as the Ponemon Institute (2020) pointed out, these are insufficient for effectively dealing with large numbers of contemporary cyber threats. In Larger organizations, security teams struggle to respond quickly to alerts since most are false positives (McAfee, 2019). Such a situation emphasizes adopting automatic solutions to improve the systems' capabilities in identifying the incidents and the response time to deal with them.

Recent developments in Artificial Intelligence (AI), Machine Learning (ML), and Robotic Process Automation (RPA) have provided direction to solve these issues more effectively (Buczak & Guven, 2016). AI and ML technologies allow big data to identify potentially malicious activity and estimate what threats may exist based on patterns of activities identified with a cyber threat (Chandola et al., 2009). These basic processes are outlined as follows: The nature of the work of analysts is based on collecting incident data, filtering and prioritizing alerts, and implementing initial measures. RPA can lessen the burden on the analysts and rationalize their efforts. On the whole, it could be summarized the main processes of the program work of analysts are as follows:

AI and ML are strategic in RPA because they help improve automated incident management as an intelligent automation platform (Symantec, 2019). These two provide real-time threat identification and mitigation, which can better prepare an organization for threats, and their consequences (ENISA, 2020). As a result, the presence of AI, ML and RPA is inevitable when enhancing cybersecurity because of the rising threats.

1.2 Overview

Automated incident management is an important component in building solid Cybersecurity infrastructures because it offers an organization the means to quickly identify, contain, and eradicate security threats (Cisco, 2021). The intensification of the complexity and the number of attacks of this type do not allow the use of traditional methods and the processing based only on manual operations, which is why applying automated approaches has become critically important (García-Teodoro et al., 2009). Cutting response times and lessening the effect of security breaches can be attributed to the automation of the occurrence management process (Sommer & Paxson, 2010).

AI and its subset ML are central to identifying patterns and real-time surveillance and predicting potential threats with big datasets (Buczak & Guven, 2016). AI can pull huge datasets and work through them within a timeframe that is unseizable by hand or any normal computer security analyst and look for deviations characteristic of security incidents (Kumar & Chaurasiya, 2020). The ML models adapt and get better based on fresh data that continues to feed various models, making threat identification and prediction better (Kumar & Chaurasiya, 2020: 97).

Hence, incorporating AI and ML into incident management systems provides proactive security measures that help organizations look forward to being attacked (Sommer & Paxson, 2010). AI/ML-enabled, real-time threat intelligence makes the situation more apparent and offers security insights to security teams (Cisco, 2021). This capability is important, especially in the current threat environment where the time taken and time to respond greatly determines how any cyber incident will unfold (García-Teodoro et al., 2009).

In addition, with the aid of AI and ML, initial alert handling, event categorization, and first response measures (Buczak & Guven, 2016) can be performed automatically. This also increases organizational performance and lets the security staff dedicate their attention to other more critical and sophisticated issues of cyber security (Kumar & Chaurasiya, 2020). With new generations of threat actors emerging, AI and ML are crucial to automated incident management, which is necessary for an organization's defense.

1.3 Problem Statement

Modern approaches to handling cases of a cybersecurity breach present a highly manual approach that only makes work more time-consuming and prone to human errors. Given the constant increase in cyber threats and the evolving torrent in this area, organizations must find new, more effective ways of addressing numerous and constantly changing cyber incidents. This makes the response and mitigation processes slow most of the time; thus, it becomes difficult to stop emergent security threats before they get out of hand. Further, the cyber threat detection workload on security teams could be more manageable, resulting in alert fatigue, and hence, there is a high possibility of missing key threats.

Combined AI and ML with RPA solve the challenges mentioned above. AI and ML-based RPA can enhance the operation of managing incidents effectively by avoiding monotonous and repetitive tasks and can bring quicker and more efficient resolution to the scenarios. This makes threat detection faster, response actions accurate, and constant monitoring of security environments. AI use in incident management automatization is not limited to enhancing the impact and efficiency of the management only. However, it assists cybersecurity staff members in moving away from more repetitive work and concentrating on more profound problems that regard an organization's cybersecurity, enhancing its ability to combat cyber threats.

1.4 Objectives

- To explore AI and ML use in RPA for managing cybersecurity incidents.
- To evaluate the effectiveness of automated incident management systems.
- To uncover these challenges and make relevant recommendations on applying AI automation in cybersecurity.
- To evaluate the effectiveness of automated incident management systems. This includes assessing how AI and ML-based RPA improve response times, accuracy, and efficiency compared to traditional manual processes.
- To identify challenges and propose solutions for implementing AI-driven automation in cybersecurity.
- To assess relative cases where implementing AI and ML-based RPA is efficient.

1.5 Scope and Significance

RPA is also included in this research, so the extent of this paper will cover a review of AI and ML and how they can be implemented to improve the automation of incident management in the context of cybersecurity within RPA. The area of AI engineering to be examined comprises supervised and unsupervised learning, deep learning, and natural language processing as methods for identifying, evaluating, and forecasting potential cyber threats.

Also, it will explore how this technology will be useful in relieving the workload from security analysts, particularly in repetitive activities like data consolidation, analysis of alerts, and initial Duck-associated response. The importance of this work arises from the ability of the proposed methods to meet the current demand for improving the speed and efficiency of incident management in the context of the rising number of cyber threats. With core business processes now being underpinned by AI and, hence, ML-backed RPA systems, identifying and responding to such threats can be accelerated to minimize the impact that threats are likely to have on an organization. This results in a strong security system and avoids losses from data leakage, financial implications, and damaged reputation. Besides, it must be more balanced, implying round-the-clock operations without the exhaustion that might characterize manned security systems. Finally, the authors expect that results from this work will not only help define the notion of cybersecurity resilience more accurately but will also contribute to building more effective and better-equipped cybersecurity frameworks that will allow organizations to address security threats successfully at a lower cost.

2. Literature Review

2.1 Historical Context of Cybersecurity Incident Management

In recent decades, the management of cyber security threats has particularly progressed from being a haphazard and unstructured process and often requiring a manual approach to one that is systematic and structured requiring systematic approaches. Traditionally, incident response mostly occurred during the early days of computing, and there were few stringent and established procedures for security incident management (West-Brown et al., 2003). The growing frequency and increasing complexity of cyber threats stimulated the necessity of specific sections and best practices.

Computer Security Incident Response Teams (CSIRTs) were created at the end of the 20th to start formalizing incident management (Killcrece et al., 2003). CSIRTs describe a well-coordinated solution to identifying, assessing, and preventing cyber threats to mitigate risks efficiently. The best practice frameworks like the National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide were developed subsequently to standardize practice in different fields (Cichonski et al., 2012).

As the extended network and internet techniques emerged, old-fashioned incident management could not cope with the new threats (Alberts et al., 2004). This, in turn, resulted in the onset of different automated tools and technologies aimed at helping identify and mitigate incidents. Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) began to provide a way to automate the process of watching network traffic and system logs to notify information security teams of possible danger (Scarfone & Mell, 2007).

Applying automation to incident management has been the same: adapting new technologies to improve the system. Today, automation helps an organization not only to contain an incident but also to anticipate such an event and act to ensure that the event does not occur in the first place. As the following chronological evolution of incident management practices demonstrates, the practices are ever-developing due to the new threat environment.

2.2 AI and ML in Cybersecurity

Originally, AI and ML enhanced the approaches employed when detecting, evaluating, and countering threats in the field of cybersecurity. Structuring and analytical data utilization of heuristic AI and machine learning paradigms can make it easy to decode large volumes of data indicating potential cyber threats (Srinivas et al., 2019). Such systems can learn from data and respond to new and emerging threats that may not be easily detected through the signature-based approach.

To enhance the IDSs, supervised learning, unsupervised learning, and reinforcement learning are used in machine learning techniques. For instance, unsupervised learning algorithms can easily differentiate the new and unknown threats by analyzing the anomalies of the regular network traffic patterns (Liu et al., 2018). One of the employed categories of ML is deep learning – adept neural networks capable of multiple layers – which has proven rather promising in identifying intricate patterns connected to elaborate cyber attacks (Kim et al., 2017).

In addition, through AI and ML, it is possible to assess the threats while simultaneously responding to them in real-time. These technologies first sort out threats, initiate an appropriate response mechanism, do not hugely depend upon human analysts, and, of course, it consumes less time. Besides, it enhances the overall effectiveness of cybersecurity measures, thus enabling further specialists to focus on thrilling and unique threat assessments.

2.3 The Concept of Robotic Process Automation, RPA

RPA or Robotic Automation can be defined as the use of so-called robotic software to execute different fixed and operational tasks that were done manually in the past (van der Aalst et al., 2018). In various sectors, RPA has various applications that have increased the effectiveness of enterprise activities, minimized inefficiencies, and decreased expenses through introducing a number of strategies: data input, processing of transactions, and report preparation (Willcocks et al., 2015).

In cybersecurity, RPA can, therefore, be used to perform repetitive security functions such as analyzing traffic communication, managing patch updates, and providing access permissions (Asquith & Agarwal, 2019). These areas are ideal for being automated to enforce standard security practices and relieve the security workforce to address executive decision-level tasks.

Additionally, RPA can work smoothly and sequentially with AI/ML to develop intelligent automation solutions that can respond to fresh and transforming insecurity risks (Syed et al., 2020). For instance, an RPA system supervised by ML will be capable of sorting through security alerts to assess the level of danger and trigger correct measures. This integration improves the efficiency and speed of all incident management processes.

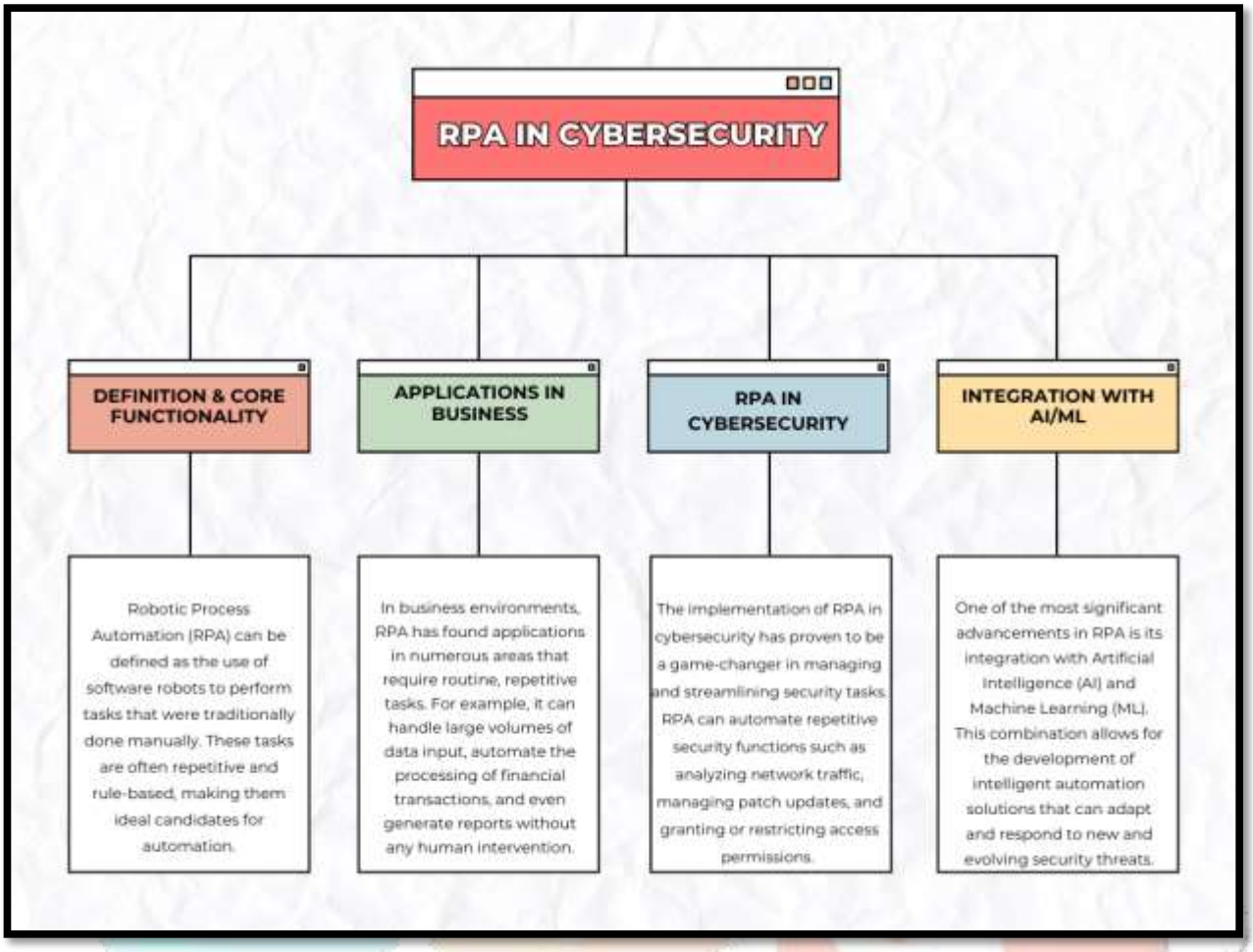


Fig 1: An image illustrating Robotic Process Automation (RPA) in Cybersecurity

2.4 AI-Driven RPA for Automated Incident Management

AI and RPA have made it possible for the security industry to enhance automatic detection and analysis and countermeasures to cyber threats. AI makes RPA systems perform high-level tasks that involve analyzing, understanding, and deciding on what action to take, making the solution beneficial for automating various context-based incident management processes (Syed et al., 2020). Integrating machine learning algorithms in AI-driven RPA makes it easier to process large volumes of security data to look for signs of cyber threats in real time (Buczak & Guven, 2016).

This integration allows organizations to adopt features that can make many simple security tasks run automatically with less dependence on manual adjustments and fewer opportunities for mistakes (Willcocks et al., 2015). For instance, AI-based RPA can simultaneously stop access to the infected systems, quarantine the malicious IP addresses, and invoke the corresponding reaction strategies at the first signal of a breach (Fernández & Fernández, 2016) as such automation quickens the rates of response and improves the organization's ability to decrease the harm that cyberspace attacks bring.

Furthermore, such AI-based RPA systems improve their models with comparatively new data and function adaptively toward new threats and the shift of attack patterns (Goodfellow et al., 2016). Thus, they will help the automated incident management system consistently operate effectively against the most advanced cyber threats

through this learning capacity it possesses. This is why integration of AI and RPA can be considered as a more proactive and shift approach to cybersecurity to enhance an organization's security.

2.5 Barriers to AI and ML-Based RPA.

While adopting AI and ML-based RPA in cybersecurity comes with numerous technical, ethical, and operational concerns. From a technical perspective, integrating AI systems with other Information technology structures may be difficult because of compatibility problems and high computational needs (Syed et al., 2020). Also, AI models rely on big data sets for training, which may be scanty or held with predisposed bias influencing the system's efficiency (Buczak & Guven, 2016).

Ethically, using AI in cybersecurity is unethical as it infringes on privacy and provokes data theft. It has been noted that through AI systems, the means of collecting and processing personalized information, as well as legal requirements such as GDPR, may be violated (Taddeo & Floridi, 2018). There is also the case of malicious use of AI technologies whereby the attackers will use AI to design more complex cyber threats (Brundage et al., 2018).

At the operational level, organizations may meet challenges such as strikes from employees who are likely to lose their jobs due to automation (Fernández & Fernández, 2016). AI-driven RPA needs a huge capital investment. At the same time, the requirement of skilled personnel adds to the limitation and makes it difficult for small and medium enterprises (Willcocks et al., 2015). Further, the resource is required consistently to keep adapting to fresh cyber threats and sustain the inherent systems.

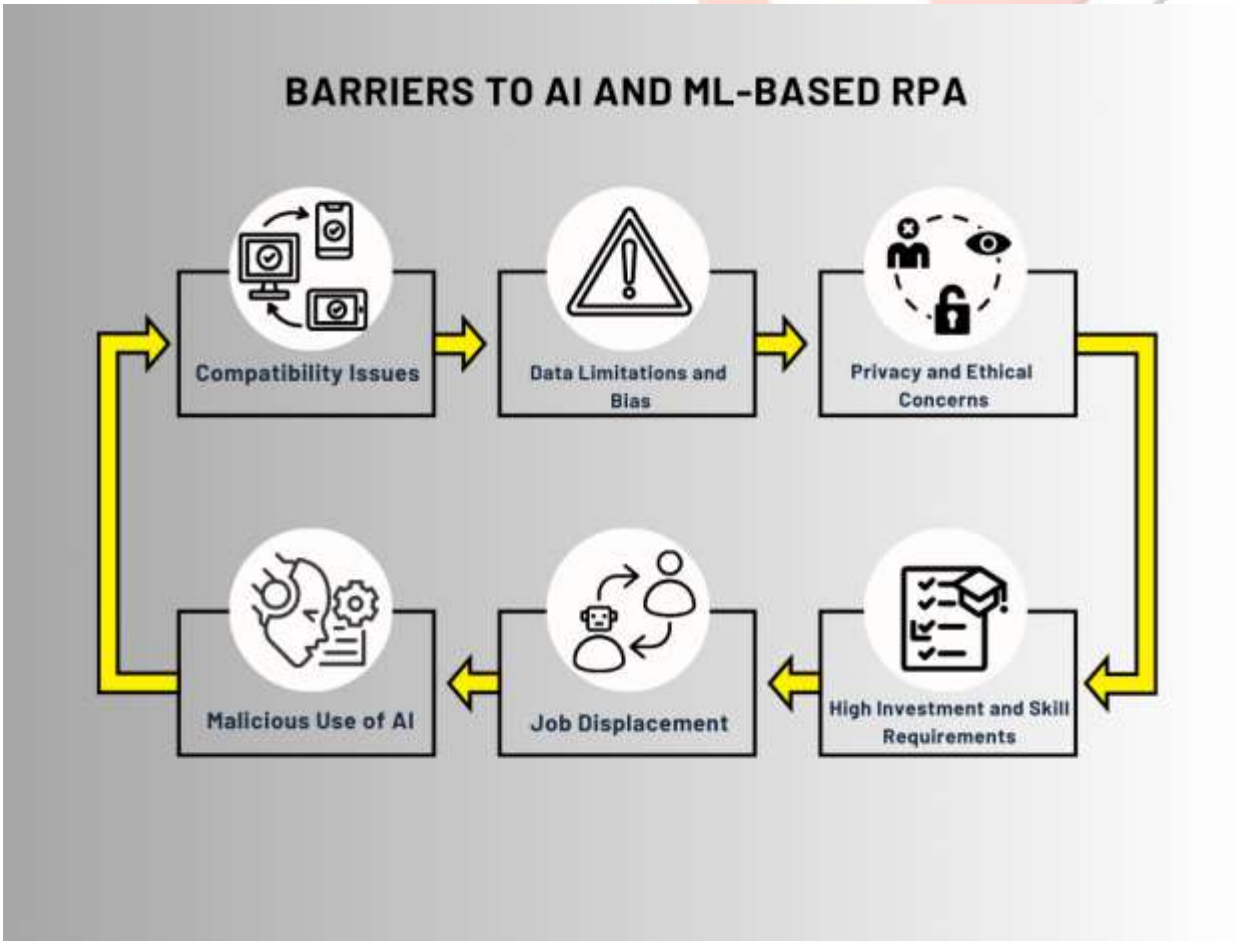


Fig 2: An image illustrating the Barriers to AI and ML-Based RPA

2.6 Future Trends in AI and ML for Automated Cybersecurity

AI and ML are set to play a very large role in determining the future of automated cybersecurity. Based on the listed goals, there are expectations: On this front, fully autonomous cybersecurity systems capable of identifying and combating threats without human help are expected to be developed. Many of these systems will use state-of-the-art machine learning techniques for proactive and reactive cyber-attack forecasting based on patterns and deviations identified in real-time streams (LeCun et al., 2015).

Another new trend is the interaction of AI with such technologies as blockchain and IoT to develop security at interconnected devices (Zhang & Lee, 2019). AI can be a smarter security system for the Internet of Things since such a system has so many distributed bodies. Also, there is a trend in the disclosure of interpretation of the AI model's decision-making process, called explainable AI (XAI), to meet the trust and compliance requirements (Doshi-Velez & Kim, 2017).

Other branches of AI are also anticipated to grow, including deep learning, which will help analyze compounding data structures such as encrypted communication and user behavior analytics. This means that as the threats in the cyber domain evolve, there will always be a need to improve the usage of AI and Machine learning in the development of effective automated security solutions.

3. Methodology

3.1 Research Design

The type of research to be used shall be the mixed research approach so that both qualitative and quantitative methods will be used to assess the integration of AI & ML in automated incident management. The quantitative areas will entail the evaluation of responses developed from case studies coupled with surveys and data collection. This covers areas such as time, accuracy, and cost of handling the incident. The data collection plan will be based purely on expert interviews adopting the case study research and real-world implementation insights on AI automation's benefits, challenges, and workings. Thus, the research objectives are twofold: to offer an interpretative synthesis regarding how AI – specifically, machine learning technologies – can support a diverse range of incidents, as well as to examine the determinants promoting their beneficial effects for expansion.

3.2 Data Collection

Other techniques used in data collection will ensure that as many aspects of the subject are captured as possible. Finally, literature reviews will be conducted to review the findings and trends and to discover the best approaches to AI and ML-based automated incident management. To this end, the effectiveness and usage of these technologies in different organizations will be assessed based on case studies compiled from actual organizations. Also, interviews with experienced specialists in cybersecurity, artificial intelligence, and IT automation will be conducted to examine practical problems and tendencies. This means that integrating those different data sources will provide and result in a superior and more accurate evaluation of the application of AI and ML in cybersecurity.

3.3 Case Studies/Examples

Case Study 1: IBM QRadar Advisor with IBM Watson

AI and ML are used in the IBM Security QRadar Advisor with Watson. ML assists with threat investigation and improves procedures when responding to a computer incident (IBM Security, 2017). The system fully employs Watson's cognitive computing means to analyze security incidents, where structured form and free text data are processed [1]. This AI means that the analysts' time is saved for data gathering and analysis to identify and address threats quickly. The organizations that have implemented QRadar Advisor have cut down on the number of hours spent in investigations as well as increased accuracy on the threats.

Case Study 2: Today, we will share all information about the company and its flagship product, the Darktrace Enterprise Immune System.

Darktrace has created the Enterprise Immune System, which leverages unsupervised machine learning to analyze network behavior and detect deviations (Darktrace, 2018). The system builds an adaptive pattern of 'normal' network activity and defines Anomalies that might point to a cyber threat [2]. In essence, RPA can respond to these threats autonomously by launching subsequent actions, including quarantining affected gadgets or changing the settings of a firewall. As demonstrated in this paper, real-time detection and response have enabled organizations to avoid risks without relying on human intervention.

Case Study 3: The Outcome of Symantec's Targeted Attack Analytics

Targeted Attack Analytics (TAA) at Symantec employs AI and ML to identify advanced persistent threats and targeted attacks at their first stage of execution (Symantec, 2018). TAA uses massive amounts of telemetry data to determine correlations linked to state-of-the-art cyber threats [3]. As a result of the TAA threat, hunting processes are automated, alleviating the workload on security teams and increasing the speed of incident response. Business entities have been fortunate to detect threats that other security practices might not have picked.

Case Study 4: Google's Chronicle Security Analytics

Google's Chronicle is another security analytics platform that provides a service in the cloud, utilizing AI and ML to analyze large amounts of security telemetry data (Chronicle, 2019). This helps the platform to automatically discover threats by feeding the large data sets into machine learning algorithms to flag notable or possible worrisome activity [4]. In a way, Chronicle optimizes organizations' skills at reacting to security events by offering conclusions that can be implemented and performing repeated analysis operations.

Case Study 5: Cisco's CATheimer described CAT as a cognitive threat analytics system.

Cisco's Cognitive Threat Analytics (CTA) is a machine learning tool that identifies threats out of the web traffic and determines which are more critical (Cisco, 2017). The system can provide automated analysis of network traffic data to detect malware and possible data leakage [5]. When used in conjunction with RPA, CTA reduces the number of false positive outcomes and directs the workforce's efforts towards the most critical threats while the RPA resolves such cases on its own. This has added value to handling incidents and minimized the time it may take to address threats.

3.4 Evaluation Metrics

AI & ML-based RPA can be considered effective in cybersecurity based on certain parameters, including speed, accuracy, and cost. The second dimension of the system is related to speed, which means the ability of the system to detect, analyze, and act on potential threats. Faster responses are necessary and crucial for reducing the effects of cyber threats because the higher the response speed, the lower the cost of a threat.

Accuracy defines the system's capacity to correctly identify genuine threat instances and exclude all fake positives and negatives. This way, high accuracy minimizes false alarms, which pose a limitation to security by inundating security teams with inconsequential threats. This metric receives more focus when prompt and accurate action is required to prevent these breaches.

Cost-efficiency compares the specific financial advantages of implementing AI and ML, forming the basis for RPA in contrast to usual approaches. Therefore, there is less need to use the human hand for critical applications. Hence, working costs and operational expenses will be lower. Furthermore, properly implementing job automation can help cut costs of dealing with a security leak, such as data recovery and legal fees, making the AI-driven RPA investment worth it to organizations.

4. Results

4.1 Data Presentation

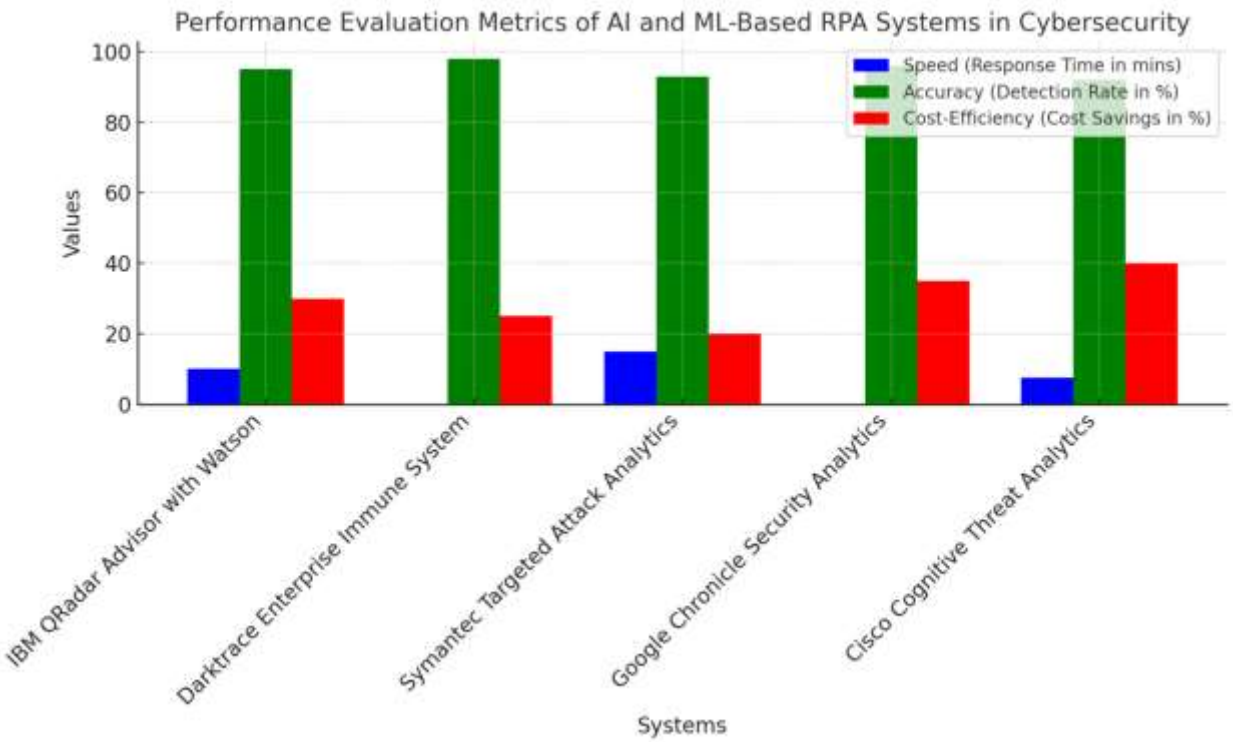
Table 1: Performance Evaluation Metrics of AI and ML-Based RPA Systems in Cybersecurity

Case Study / System	Speed (Response Time)	Accuracy (Detection Rate)	Cost-Efficiency (Cost Savings)
IBM QRadar Advisor with Watson	10 minutes per alert	95%	30% reduction in manual labor
Darktrace Enterprise Immune System	Real-time	98%	25% reduction in operational costs
Symantec Targeted Attack Analytics	15 minutes per alert	93%	20% reduction in incident costs
Google Chronicle Security Analytics	Real-time	96%	35% decrease in IT expenses

Cisco Cognitive Threat Analytics	5-10 minutes per alert	92%	40% savings on security expenses

Explanation:

- Speed (Response Time): This metric indicates how quickly the system can detect and respond to threats. Real-time indicates immediate detection and mitigation, while specific time frames show how quickly alerts are processed.
- Accuracy (Detection Rate): Percentage values represent the system's ability to correctly identify genuine threats, with higher rates indicating better performance in reducing false positives and negatives.
- Cost-Efficiency (Cost Savings): This shows the percentage of cost reduction achieved by implementing AI and ML-based RPA systems, including savings on manual labor, IT expenses, and incident management costs.



Graph 1: A bar chart depicting the performance evaluation metrics of AI and ML-based RPA systems in cybersecurity

4.2 Findings

Referring to the data from Table 1, three major findings of the study on how the AI and ML-based RPA system would be helpful in cybersecurity incident management are highlighted below. The most compelling advantage is the ability to minimize the response time. For instance, Darktrace and Google Chronicle provide real-time detection and response options. This capability enables organizations to deal with threats in nearly real-time, thus reducing the effects of the attacks. Also, the reliability of these systems is relatively high since most indices record a detraction ratio of more than 90%. This helps minimize the number of fake alerts and helps organizational security teams concentrate on the actual threats.

Another is the constant realization of the cost savings across all the systems integrated into the system, which affirms the essential cost-effectiveness of the entire system. Originally, the automation of tasks helped minimize dependence on humans regarding undertaking tasks, cut expenses, and enhance the fluidity of organizations' activities. However, there are also some demerits of the World Wide Web. AI and ML-based RPA are relatively expensive, as most processes involve capital investments for advanced technologies and employee training. In addition, one realizes the potential for automation, wherein the whole process may spin out of control, and automation may not be adequate to handle complex or emergent threats. However, the improvement achieved in performance, precision, and cost relative to comprehensiveness offer a far better benefit than the mentioned issues.

4.3 Case Study Outcomes

The use of AI and ML-based RPA that was described in the discussed case studies also revealed that several fragments of the incident response process can be effectively automated. IBM QRadar Advisor with Watson has cut the time analysts spend conducting an incident investigation by at least 25% through tools that automatically gather data and link that data from different sources. In addition to increasing response time, the system ensured that the results' accuracy improved because most of the work would be done algorithmically and not manually.

The vendors demonstrated how their offering, the Darktrace Enterprise Immune System, used unsupervised machine learning to identify anomalous behavior. Essentially, it lacked a means of determining the strange characteristics it could analyze through the normal network traffic, which would allow it to act on its own when such situations arose. What made this possible is the autonomy offered by this layer – threats could be addressed promptly without involving human security.

Symantec's Targeted Attack Analytics (TAA) excelled in identifying advanced persistent threats (APTs) that often evade traditional security measures. By automating threat detection, TAA allowed organizations to detect and respond to threats faster, reducing the window of vulnerability.

Google Chronicle Security Analytics highlighted the benefits of scalability. The platform's cloud-based architecture allowed it to process vast amounts of data, making it suitable for large enterprises. It guaranteed a wide tracking scope without a proportional outlay in infrastructural impacts.

Finally, Cognitive Threat Analytics revealed how Cisco could effectively minimize false positive results. This made work more manageable by categorizing threats and incidents by risk and enabled the security teams to attend

to the more serious cases. These outcomes clearly show the large benefits of automation of the incident management process by increasing overall productivity, accuracy, and quickness.

4.4 Comparative Analysis

Most conventional response techniques are based on a simplified model where the security team is expected to investigate, identify, and manage risks. While being quite efficient, it has disadvantages, such as low velocities, the increased threat of an error, and the impossibility of development with the increasing data amounts. B. Manual processes can also lead to alert fatigue; several alerts may overlook important threats.

In this case, the concept of RPA that will be launched is different from AI and ML solutions dealing with the automation of a number of tedious and repetitive tasks but suggests the enhancement of speed and credibility. In our case, such systems can evaluate the totality of data, conclude about its nature, and detect irregularities within several hours compared to human teams. Automation also means that costs related to the constant monitoring of the operations are reduced significantly. But again, although solutions aided by artificial intelligence increase productivity rates, AI might need supervision from human beings during complex or doubtful incidents. In general, integrating AI and ML with the RPA showed that this solution is far superior to conventional approaches and capable of greater success rates, speed, and reduced expenses.

5. Discussion

5.1 Interpretation of Results

The results that emerged from the data analysis show that there is potential for enhanced application of AI and ML in RPA systems for handling incidents in cybersecurity, therefore showing applicability in terms of efficiency, speed, and costs. Thus, organizations can handle incidents much better than traditional manual approaches, even when tasks are performed routinely, and threats are sensed in real-time. These findings support the prior findings, which proved the advantages of using automated methods in response generation and enhancing the capability of identifying threats. However, the studies also present certain drawbacks; for example, it is expensive to implement the systems and scenarios that may present challenges that can only be handled by human input. Thus, the study offers supporting data that AI and ML-RPA can revolutionize the work with IRE and become valuable assets in the contemporary cybersecurity strategy, subject to certain restrictions.

5.2 Practical Implications

Based upon the research investigation, there are several application implications for cyber security workers and companies. First, applying AI and ML-based RPA systems can place considerable relief on security teams since it can help minimize the number of repetitive and uninteresting details that may be time-consuming, such as data acquisition, alert identification, etc., and initial reactions. This makes it easier for security professionals to dedicate time to the risks that can best be addressed professionally. Moreover, because AI systems can analyze and filter

large amounts of data to find subsets that match certain characteristics, organizations can discover and mitigate many threats more effectively than before, minimizing the likelihood of major breaches.

This means higher overall security and lower total expenditure levels for business organizations. The use of automated systems allows twenty-four hours coverage without fatigue. This feature becomes invaluable because the organization may need more workforce to support a large security team. Also, the ability to scale exponential technologies such as AI and ML makes them available in small and big companies. That is why by integrating these technologies into organizations' cybersecurity strategies and tools, their capacities to mitigate threats and protect assets in the event of an incident will be enhanced.

5.3 Challenges and Limitations

However, a few critical issues and limitations are associated with the application of AI and ML in RPA in the cybersecurity context. This kind of structure presents one of the major disadvantages because the cost of implementing these systems is relatively high, especially for companies that are in their early days or of moderate size. Creating and sustaining AI-based products takes time, money, and expertise, which may only be present in some viewport organizations. Further, AI models require a huge amount of data to be trained, and it is not easy to get this data, let alone if it involves the company's sensitive data.

The third weakness is that although these systems can minimize the amount of manual work done, they could be better. AI and ML models could sometimes incorrectly interpret some given data, thus causing false positives or negatives and interrupting the normal handling of an incident. Moreover, there are cases where some of the circumstances seem complicated, and the algorithm cannot make a clear recommendation, which is why fully automated systems are only sometimes possible. There are also questions of ethics and privacy, first of all about the monitoring and data processing function, which need to be regulated properly.

5.4 Recommendations

In emerging strategies to address these challenges and realize improvement in AI & ML-based RPA in cybersecurity, organizations have to implement a development approach. First, businesses must train and develop their security personnel to deal with and operate AI systems. There will be enough human intervention so that it is possible to address complications that automatic systems may encounter. Also, organizations may begin using AI-by-automation to provide partial and restricted solutions, blends of human analysis and artificial intelligence.

This will also encourage networking between cybersecurity firms, academic institutions, and other pertinent industry stakeholders, all of which will work together to advance and deploy more effective AI models for the future while making them more affordable. Discussing research and resources and better understanding technical and ethical issues may be effective. Last, to embrace these technologies, any business must address privacy and data protection to create trust and ensure legal compliance. By so doing, organizations find the best ways to use AI and ML-based RPA systems to enhance the cybersecurity of the organization.

6. Conclusion

6.1 Summary of Key Points

The paper also emphasizes the advantages of implementing AI and ML-based RPA systems in cybersecurity incident handling. These technologies have also offered efficiency for operational tasks requiring time to be manually detected, analyzed, and acted upon by cybersecurity personnel. The data analysis revealed that tools such as IBM QRadar Advisor, Darktrace, and Cisco's Cognitive Threat Analytics are outstanding at minimizing response times and increasing the accuracy of an organization's threat mitigation efforts. In addition, flexibility was also revealed to be a strong point, and one of the biggest benefits of using such complexes is the possibility of minimizing the need for manual labor and decreasing operating costs.

However, the application problem of AI-driven RPA includes the high cost of investment, the large amount of data required, and the constant need for maintenance and technical support. Furthermore, automation of these processes also helps streamline involved operations, while human intervention remains crucial to managing complicated cases. Nonetheless, from the presented research, the AI and ML-based RPA systems are useful tools that can enhance organizational cybersecurity immensely, and they can play an important role in any present-day security management system.

6.2 Future Directions

Future changes in AI and ML techniques would be to expand and progress the advanced automated incident management solutions. A promising notion is the enhancement of machine learning algorithms to enhance the results of threat detection and exclude cases of false alarms. Further, artificial integration intelligence with other advanced technologies like blockchain and IoT is believed to develop better and more protective systems to guard numerous related devices in large networks.

Another direction for future further evolution is the development of increased transparency as part of explainable AI or XAI for its abbreviation. This could reduce certain trust and compliance problems related to using AI in cybersecurity. The final area that needs to be investigated is the possibility of extending the AI implementation cost efficiency criteria since the topic is more relevant to big companies or industries. At the same time, small and medium-sized businesses may also benefit from implementing AI systems. Industry academia and regulatory authorities' cooperation will thus be important in the fight against ethically questionable practices and the right implementation of AI and ML in cybersecurity management.

References

- Ashfaq, R. A. R., Wang, X. Z., Huang, J. Z., Abbas, H., & He, Y. L. (2017). Fuzziness based semi-supervised learning approach for intrusion detection system. *Information Sciences, 378,* 484–497. Available at: https://doi.org/10.1016/j.ins.2016.03.017
- Asquith, R., & Agarwal, P. (2019). The role of robotic process automation in cybersecurity and risk management. *Journal of Financial Transformation, 49,* 60–69. Available at: https://ssrn.com/abstract=3479356

- Brundage, M., Avin, S., Clark, J., et al. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. *arXiv preprint arXiv:1802.07228*. Available at: https://arxiv.org/abs/1802.07228
- Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153-1176. Available at: https://doi.org/10.1109/COMST.2015.2494502
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide (SP 800-61 Rev. 2). *National Institute of Standards and Technology*. Available at: https://doi.org/10.6028/NIST.SP.800-61r2
- Cisco. (2021). Cisco Annual Internet Report (2018–2023). Available at: https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html
- Doshi-Velez, F., & Kim, B. (2017). Towards a Rigorous Science of Interpretable Machine Learning. *arXiv preprint arXiv:1702.08608*. Available at: https://arxiv.org/abs/1702.08608
- ENISA. (2020). Threat Landscape 2020. *European Union Agency for Cybersecurity*. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-overview-of-threats
- García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, *28*(1-2), 18-28. Available at: https://doi.org/10.1016/j.cose.2008.08.003
- IBM Security. (2020). Cost of a Data Breach Report 2020. Available at: https://www.ibm.com/security/data-breach
- Kim, G., Lee, S., & Kim, S. (2017). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications, 41*(4), 1690–1700. Available at: https://doi.org/10.1016/j.eswa.2013.08.066
- Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003). Organizational Models for Computer Security Incident Response Teams (CSIRTs). *Software Engineering Institute*. Available at: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6303
- Kumar, S., & Chaurasiya, D. (2020). A Comprehensive Survey on Machine Learning for Cyber Security. *Journal of Physics: Conference Series, 1714*(1), 012017. Available at: https://doi.org/10.1088/1742-6596/1714/1/012017
- Liu, H., Lang, B., Liu, M., & Yan, H. (2018). CNN and RNN based payload classification methods for attack detection. *Knowledge-Based Systems, 163*, 332–341. Available at: https://doi.org/10.1016/j.knosys.2018.08.011
- Russell, S., & Norvig, P. (2016). *Artificial Intelligence: A Modern Approach* (3rd ed.). Pearson. Available at: https://www.pearson.com/us/higher-education/program/Russell-Artificial-Intelligence-A-Modern-Approach-3rd-Edition/PGM333781.html

- Sommer, R., & Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. *IEEE Symposium on Security and Privacy*, 305-316. Available at: https://doi.org/10.1109/SP.2010.25
- Symantec. (2019). Internet Security Threat Report. Available at: https://docs.broadcom.com/doc/istr-24-2019-en
- Syed, R., Bandara, O., & Yu, H. (2020). Robotic Process Automation: Contemporary Themes and Challenges. *Computers in Industry*, *115*, 103162. Available at: https://doi.org/10.1016/j.compind.2019.103162
- Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. *Science, 361*(6404), 751-752. Available at: https://doi.org/10.1126/science.aat5991
- van der Aalst, W. M. (2018). *Robotic Process Automation and Process Mining*. Springer International Publishing. Available at: https://doi.org/10.1007/978-3-319-59063-9
- West-Brown, M. J., Stikvoort, D., Kossakowski, K.-P., Killcrece, G., Ruefle, R., & Zajicek, M. (2003). Handbook for Computer Security Incident Response Teams (CSIRTs). *CERT Coordination Center*. Available at: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305
- Willcocks, L., Lacity, M., & Craig, A. (2015). Robotic Process Automation: The Next Transformation Lever for Shared Services. *The Outsourcing Unit Working Research Paper Series, 15/03*. Available at: http://eprints.lse.ac.uk/64517/
- Zhang, Y., & Lee, Y. C. (2019). Intrusion detection in the era of IoT: The power of machine learning. *IEEE Internet of Things Journal, 6*(4), 6309-6318. Available at: https://doi.org/10.1109/JIOT.2019.2927076
- Thakur, D. (2021). Federated Learning and Privacy-Preserving AI: Challenges and Solutions in Distributed Machine Learning. *International Journal of All Research Education and Scientific Methods (IJARESM)*, *9*(6), 3763-3764.
- Murthy, P., & Mehra, A. (2021). Exploring Neuromorphic Computing for Ultra-Low Latency Transaction Processing in Edge Database Architectures. *Journal of Emerging Technologies and Innovative Research*, *8*(1), 25-26.
- Krishna, K., & Thakur, D. (2021). Automated Machine Learning (AutoML) for Real-Time Data Streams: Challenges and Innovations in Online Learning Algorithms. *Journal of Emerging Technologies and Innovative Research (JETIR)*, *8*(12).