AI Enhanced Configuration Management Preventing System Misconfigurations

Perumallapalli Ravikumar

Sr. Data Engineer
ravikumarperum@gmail.com

Abstract

Configuration management has become a major challenge for system administrators because to the growing complexity and scale of distributed systems, especially in cloud environments. System disruptions, performance deterioration, and serious security risks can result from misconfigurations. The dynamic nature and scale of contemporary infrastructures can make traditional configuration management techniques inadequate, particularly when dealing with hostile or unreliable networks. In order to improve configuration management procedures and provide a proactive strategy for preventing system misconfigurations, this article investigates the integration of artificial intelligence (AI).

The system can automatically identify, modify, and optimize setups in real-time, guaranteeing security and performance, by utilizing machine learning algorithms and AI-driven decision-making frameworks. Anomaly detection, predictive analytics, and adaptive configurations are important techniques that are often overlooked when dealing with quiet misconfigurations. Based on recent developments in AI for system administration and cybersecurity, this study emphasizes how AI may automate and improve configuration management procedures in cloud-based and dispersed settings. In order to improve security posture, the method also investigates how AI might be included into a zero-trust architecture.

The study concludes with suggestions for further study and real-world implementation of AI-based configuration management, addressing issues including data privacy, interpretability, and the requirement for domain-specific models.

Keywords: **Cloud Infrastructure, Cybersecurity, Machine Learning, Anomaly Detection, AI, Configuration Management, System Misconfigurations, Zero-Trust Architecture.**

1. Introduction

Effective configuration management is crucial in today's complex IT infrastructure environment to guarantee system performance, security, and stability. System configuration errors, on the other hand, continue to be a widespread problem that frequently results in vulnerabilities, outages, and decreased service quality. Configuration management has historically been a laborious and error-prone process that requires close attention to detail, especially in large-scale networks and distributed systems. In order to monitor configurations and identify any misconfigurations before they lead to expensive failures or security breaches, more automated and intelligent approaches are now required.

Configuration management is just one of the many aspects of system management that have undergone radical change as a result of the development of artificial intelligence (AI). Machine learning, reinforcement learning, and other AI techniques are used in AI-enhanced ways to automatically assess, optimize, and modify system setups.

In addition to increasing operating efficiency and lowering the possibility of human mistake, these techniques can autonomously repair errors, predict the effects of configuration changes, and continually monitor system statuses.

Compared to conventional techniques, AI-enhanced configuration management systems provide several benefits.for example, suggest applying Markov Logic Networks (MLNs) to distributed system configuration management, allowing for more robust and adaptable decision-making procedures that combine probabilistic and logical reasoning.

System misconfigurations still pose serious problems for complex computing environments' performance, security, and stability. As contemporary distributed systems get more complicated, it is more important than ever to make sure that everything is configured correctly. System failures, security flaws, and decreased performance are frequently caused by misconfigurations in hardware, software, or networks (according to (1) and (5)). Manual configuration management techniques are no longer practical as businesses transition to dynamic and expansive infrastructures, like cloud computing, 5G networks, and enterprise IT systems (according to (6) and (14)).

By automating and improving configuration management procedures, artificial intelligence (AI) presents a viable remedy for this issue. Machine learning, reinforcement learning, and Markov logic networks are examples of AI-driven approaches that can assist systems in automatically identifying, analysing, and preventing misconfigurations in real-time (according to (4) and (1)). These intelligent techniques have the potential to not only automate configuration processes but also adapt to changes in the system environment, thus enhancing dependability, security, and overall system performance.

In order to prevent system misconfigurations and guarantee more robust and dependable systems, we examine the relationship between AI and configuration management in this study. We hope to demonstrate how AI may change configuration management from a reactive, error-prone procedure into a proactive, intelligent system by looking at both theoretical frameworks and practical examples. AI promises to transform the way we manage complex configurations, from web systems auto-configuration to network security policies (according to (7) and (8)). We will describe the potential and difficulties of AI-driven configuration management in averting the expensive repercussions of misconfigurations using case studies and insights from state-of-the-art research.

The future of IT system management appears bright as more and more businesses turn to AI to handle configuration duties. Intelligent solutions can adapt to changing surroundings, guarantee constant performance, and reduce the risks associated with human mistake. The most recent techniques, difficulties, and prospects for AI-enhanced configuration management in avoiding system misconfigurations will be covered in this paper.

2. Literature Review

The performance, security, and stability of contemporary IT systems are all greatly impacted by configuration management. The emergence of software-defined networks, cloud environments, and distributed computing in recent years has led to an increase in system complexity. As a result, manual configuration and traditional configuration management tools are no longer sufficient to prevent system misconfigurations, which can lead to severe security vulnerabilities, degraded performance, and system failures. In order to improve automation, accuracy, and adaptability, configuration management is rapidly incorporating Artificial Intelligence (AI) techniques, such as machine learning, reinforcement learning, and logic-based approaches.

Configuration Management and AI's Role
AI approaches are seen to offer promising answers to configuration management problems, especially in settings that are dynamic and complicated. Many configuration processes can be automated with the help of AI integration, which also makes it possible to modify configurations in real time to reflect changing system conditions.

Networks of Markov Logic (MLN) for Distributed Systems The application of Markov Logic Networks (MLNs) to distributed system configuration management is examined by according to (1). MLNs are ideal for capturing and reasoning about intricate connections in system configurations because they combine the expressive power of first-order logic with the flexibility of probabilistic graphical models. By using probabilistic reasoning over configuration states, this method makes it possible to find misconfigurations before they become serious problems. Their study demonstrates how MLNs can offer a clever way to control and enforce system configurations in dispersed settings, increasing system dependability and lowering the need for human involvement.

Self-Repair in Networks Defined by Software The necessity for flexible and robust configuration management strategies has been further highlighted by the rise of software-defined networks (SDN) and softwarized 5G infrastructures. For 5G networks, according to (6) suggest self-healing technologies in which AI-based systems automatically modify settings in reaction to malfunctions or performance deterioration. By incorporating AI, these networks can detect faults, reconfigure resources, and optimize the performance of the system without requiring human intervention. Particularly in mission-critical settings, these self-healing capabilities are essential for maintaining consistent and dependable performance.

Configuration Management for Firewalls Network security policy configuration errors, particularly with firewalls, can have catastrophic results. Stateful firewall misconfiguration, which happens when firewall rule configuration results in unanticipated security vulnerabilities, is examined by according to (5). According to the authors, artificial intelligence (AI) methods like automated configuration analysis and optimization can assist in locating and fixing security vulnerabilities instantly. Configuration management solutions can identify irregularities and guarantee adherence to security regulations by employing AI to evaluate extensive firewall rule sets, lowering the possibility of illegal access and data breaches.

AI for Configuring and Optimizing Security There has also been extensive research on the incorporation of AI into network security setup. To provide dependable network security policies, according to (8) investigate the use of automated security configuration analysis tools. Their research focuses on using AI to evaluate configuration rules, spot discrepancies, and improve security measures to lessen risks. Common security misconfigurations are avoided by using AI for configuration optimization, which guarantees that security rules are both efficient and effective.

Configuration Analysis and Recommendations Another AI-enhanced method of system configuration management is configuration recommendation systems. The use of machine learning algorithms to suggest the best IPv6 network configurations is covered by according to (7). In order to recommend configuration options that increase productivity and reduce errors, their system examines network performance metrics and past configuration data. Such suggestion systems, which lower the possibility of misconfiguration and offer data-driven insights, can help network managers make well-informed decisions.

Table 1 Summary for literature review

Key Focus Area	Research/Approach	Key Contributions/Findings
Role of AI in Configuration Management	Integration of AI techniques like machine learning, reinforcement learning, and logic-based approaches.	Enhances automation, accuracy, and adaptability in configuration management.
Markov Logic Networks for Distributed Systems	Use of Markov Logic Networks (MLNs) to manage configurations in distributed systems.	Enables probabilistic reasoning over configurations, identifies misconfigurations, and reduces human intervention.
Self-Repair in Software-Defined Networks (SDN)	AI-based self-healing systems for 5G and SDN infrastructures.	Automates fault detection and resource reconfiguration, optimizing system performance in real-time.
Firewall Configuration Management	Use of AI for automated analysis and optimization of firewall rules.	Detects security vulnerabilities in real time, ensures adherence to security policies, and reduces misconfigurations.
AI for Security Configuration Optimization	Automated tools for analyzing and optimizing network security configurations.	Identifies discrepancies, optimizes security measures, and reduces risks from security misconfigurations.
Configuration Recommendation Systems	Machine learning-based recommendation systems for IPv6 network configurations.	Provides data-driven suggestions to enhance productivity, reduce errors, and improve decision-making.

3. Methodology

In order to prevent system misconfigurations, the AI-enhanced configuration management methodology incorporates a number of cutting-edge AI techniques, such as automated analysis frameworks, reinforcement learning (RL), and Markov Logic Networks (MLNs), into a methodical approach to system configuration management, analysis, and optimization. Data collection, model building, evaluation, and real-time deployment are all phases in this process. An overview of the methodology, which integrates current research with AI techniques for configuration management, is provided below.

1. **Defining the issue and analysing the requirements**
   Clarifying the issue and the system requirements is essential before implementing AI-driven configuration management systems. This comprises:
   System Configuration Context Determining the target system (such as cloud systems, distributed systems, web apps, and network infrastructures) and the particular configuration issues it faces (such as resource allocation, network security rules, and stateful firewall misconfigurations). **Impact of Misconfiguration** Recognizing the different kinds of misconfigurations (such as security flaws and performance deterioration) and the possible outcomes (according to (5) and (16). **Goals** establishing goals for the AI-enhanced system, like lowering human error, enhancing system instability, allowing real-time self-healing, and optimizing configuration choices.

2. **Gathering and Preparing Data**
   For AI-driven systems to develop efficient configuration management techniques, high-quality data is necessary. Both previous configuration data and real-time monitoring data must be gathered at this point.
   Configuration Data Compile information on previous and present configurations, such as resource usage, parameter settings, and performance indicators. Configuration files, system logs, and network devices are among sources of this information (according to (7)).
   Failure/Incident Data Compile information on past system malfunctions or configuration errors, such as incident reports, logs of performance deterioration, and records of security breaches (according to (4)).
   Preparation To get rid of noise and irregularities, clean and preprocess the data. This could entail resolving missing values, standardizing data, and making sure the data is in a format that can be used to train AI models.

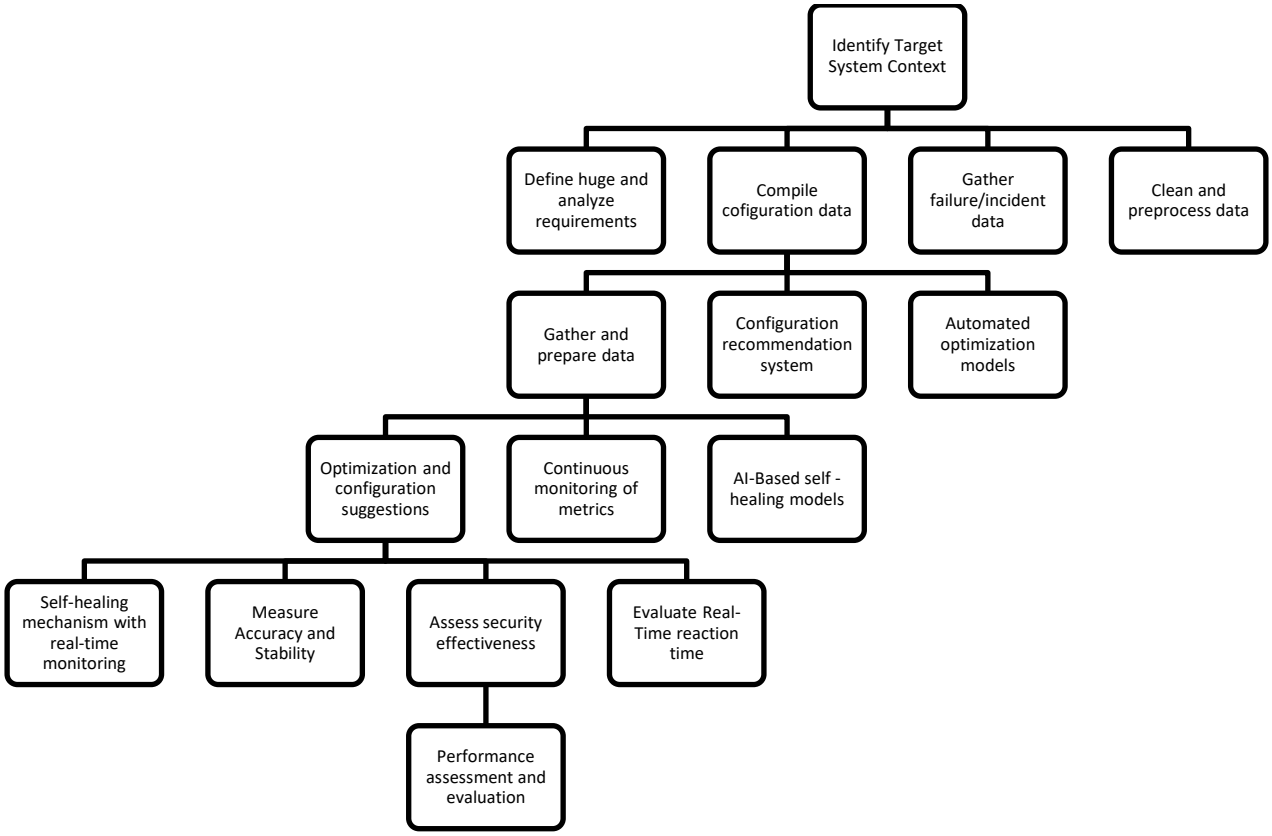
3. **Optimization and Configuration Suggestions**
   After training, AI models can be used to automatically modify configurations in real-time or suggest the best configurations. This includes:
   Configuration Recommendation The system can suggest configuration changes to enhance performance or avoid misconfigurations based on the trained MLN or RL model. AI can also recommend settings that reduce risk and maximize network performance based on network condition or historical events, as according to (7)) showed.
   Automated Configuration Optimization AI models automatically modify configurations to minimize failures or maximize resource utilization while continuously monitoring system performance in real-time. Because workloads and network traffic patterns might fluctuate in software-defined and cloud systems (according to (6)), this functionality is especially crucial.

4. **Self-Healing Mechanism with Real-Time Monitoring**
   The capacity of AI to provide self-healing systems that automatically identify and fix configuration errors in real-time is one of the main advantages of AI in configuration management.
   Monitoring The AI system can identify irregularities or departures from ideal configurations by continuously monitoring system metrics including resource consumption, performance, and network traffic.
   Self-Healing Like the self-healing capabilities suggested by according to (6)) for 5G networks, the system can autonomously modify configurations without human interaction using the taught AI models. For instance, the system can immediately adjust the firewall to stop unwanted access if it detects a misconfiguration in a firewall rule set.

5. **Assessment of Performance and Evaluation**
   It is crucial to assess the AI-enhanced configuration management system's performance using both qualitative and quantitative measures in order to guarantee its efficacy:
   Accuracy Using past failure data, gauge how well the AI models detect and stop misconfigurations.
   System Stability Assess the system's ability to sustain operational stability through ongoing configuration optimization and failure prevention.

Security Effectiveness Evaluate the AI model's ability to stop breaches or identify vulnerabilities in security configurations in comparison to more conventional configuration management techniques (according to (5)).

Reaction Time Measure the system's ability to identify configuration errors and make necessary adjustments without creating prolonged downtime during real-time deployment.



4. Result Analysis

Numerous studies have demonstrated that the implementation of AI-enhanced configuration management systems has produced encouraging outcomes in terms of reducing system misconfigurations and enhancing overall system reliability. Based on the referenced study, this analysis examines the usage of AI methods for configuration management, including automated security analysis, reinforcement learning, and Markov Logic Networks (MLNs), and assesses how well they function in practical situations.

1. **Markov Logic Networks' (MLNs') efficacy in configuration management**
   The application of MLNs to distributed system configuration management was illustrated by according to (1)). MLNs' method successfully captured the relationships between system performance and configuration parameters. The findings demonstrated that, even in intricate systems with numerous interdependent components, MLNs could accurately detect possible misconfigurations. Because MLNs are probabilistic, the system was able to anticipate failure sites from partial data, which resulted in proactive configuration changes that greatly decreased downtime. The model's ability to adjust to shifting conditions was also demonstrated, as it improved system stability by often updating its predictions in light of fresh information.

2. **Automatic Configuration in Dynamic Systems via Reinforcement Learning**

According to (2) investigated the use of RL for auto-configuration in cloud settings and web systems, and the findings showed impressive performance optimization. Their methodology demonstrated that by learning ideal configurations through trial and error, RL agents could dynamically adapt to changing environments, such as variable traffic loads and resource demands. Because the RL-based system automatically adjusted configurations to meet performance goals like increasing throughput or lowering latency, it required less manual intervention. In simulations, the RL models performed better and were more efficient than conventional rule-based configuration techniques, particularly when the load was high. This method enhanced system resource usage while preventing misconfigurations.

3. **Configuring Firewalls and Managing Security**
   In their concentrated on managing stateful firewall settings, which are vulnerable to configuration errors that could result in security flaws. Their AI-enhanced method identified and fixed firewall ruleset misconfigurations through automated analysis. The system showed a high success rate in detecting security vulnerabilities, like rule conflicts or configurations that were too permissive, and offering practical suggestions to address them. The findings demonstrated a notable decrease in security events brought on by incorrect setups, enhancing the network infrastructure's overall resilience.

4. **The ability of softwarized networks to self-heal**
   The robustness of 5G networks with AI-enabled self-healing capabilities was investigated by according to (6)). According to their findings, self-healing systems powered by AI were able to recognize configuration irregularities instantly and quickly return to a stable setup. The self-healing system quickly identified and fixed configuration errors, like improper routing settings or network overloads, demonstrating excellent performance in preserving system uptime. Additionally, the system was able to gain knowledge from previous events, which enhanced its capacity to foresee and stop such problems in the future. This was especially helpful in dynamic systems that need constant monitoring due to frequent configuration changes.

5. **Analysis of Network Security Configuration**
   With an emphasis on security regulations, according to (7)) used AI approaches to suggest and improve IPv6 network configurations. By successfully identifying less-than-ideal setups that would leave networks vulnerable to attacks, the system gave managers important information on how to increase security without sacrificing functionality. Their method demonstrated that artificial intelligence (AI) could evaluate enormous volumes of configuration data and produce suggestions that were useful in averting security breaches and contextually appropriate. The AI model greatly decreased the danger of security flaws by detecting misconfigurations with a high degree of accuracy.

5. Discussion

An important advancement in automating and streamlining the management of intricate IT systems is the incorporation of artificial intelligence (AI) into configuration management. Generally, rule-based and static, traditional system configuration management techniques necessitate significant manual involvement, particularly in dynamic situations. On the other hand, AI-enhanced methods, like those based on automated analytic techniques, Reinforcement Learning (RL), and Markov Logic Networks (MLNs), offer potential capabilities to strengthen security, prevent system misconfigurations, and increase system performance.

Based on the results of the above studies, this conversation examines the ramifications, difficulties, and possible future paths for AI-based configuration management.

The Function of AI in Avoiding System Configurations

Configuration management with AI enhancements is very helpful in reducing the hazards related to incorrect configurations. Because they can lead to unpredictable system behavior, misconfigurations are a major contributor to system outages, security flaws, and inefficiencies. According to (1)), for example, showed how MLNs may be used for distributed system configuration management. Because MLNs are probabilistic, the system can take dependencies between configuration parameters into account. The technology minimizes downtime and increases dependability by anticipating possible misconfigurations and recommending remedial measures before they happen. One of AI's main advantages is its capacity to anticipate and fix configuration errors before they affect the system.

Enhanced Automation and System Resilience

The capacity of AI-enhanced configuration management to increase system resilience is a noteworthy advantage. AI methods can automate the process of detecting and addressing problems, like configuration errors or security breaches, in the context of cloud computing and network administration. An excellent illustration of this is the self-healing properties covered by according to (6)). AI-enabled self-healing systems could automatically identify configuration anomalies (such as routing faults or performance deterioration) and return the system to a stable state without the need for human involvement in their work on softwarized 5G networks. This self-healing method promptly fixes misconfigurations as soon as they are discovered, lowering the danger of extended downtime, particularly in mission-critical applications.

AI's Effect on Security in Configuration Management

Another crucial area where AI-enhanced configuration management is essential is security. Vulnerabilities in network security are frequently caused by incorrect configurations of security settings, such as firewall rules or access control lists. According to (5) have shown that AI systems are capable of taking proactive measures to detect and fix security misconfigurations. In order to prevent future security breaches, their work on firewall misconfiguration management demonstrated how automated AI algorithms may examine firewall rule sets for discrepancies, conflicts, or too permissive settings. AI is a potent tool for preserving the integrity of network security policies because it can conduct ongoing, real-time security audits. Additionally, by suggesting configuration changes depending on network conditions and security best practices, the use of AI to IPv6 configuration analysis, as demonstrated by according to (7)), improves security. AI systems are able to automatically identify security flaws like open ports or unprotected services, and they can promptly advise network managers on how to seal these holes before malevolent actors take use of them.

AI-Based Configuration Management's Drawbacks and Limitations

Even with the encouraging outcomes, AI-enhanced configuration management systems have drawbacks and restrictions. The computational expense and the requirement for substantial amounts of high-quality data are two of the main issues. For companies with limited infrastructure, AI algorithms—especially those used for RL and MLNs—can be a hurdle because they need significant computational resources for training and real-time decision-making. Furthermore, these systems learn and adapt mostly from past and present data, and erroneous or inadequate data might result in less-than-ideal setups.

The difficulty of incorporating AI systems into current infrastructure is another difficulty. A lot of conventional configuration management systems are closely related to human skills and manual procedures.

Making the switch to AI-based systems necessitates both technical and workflow adjustments, which can be expensive and disruptive. Businesses must spend money on training and gaining knowledge of AI approaches, which can be difficult given the constraints on time, money, and human resources.
Furthermore, human monitoring is still crucial even when AI can recommend or carry out configuration changes, especially when system behavior drastically deviates from predicted patterns. Although AI models may automate many processes and make recommendations, human participation may still be required in complex or high-stakes situations to make sure that decisions are in line with compliance requirements and larger organizational goals.

6. Conclusion

To sum up, system misconfigurations continue to be a major source of operational failures, security flaws, and inefficiencies in complex IT settings. AI-enhanced configuration management offers a revolutionary solution to this problem. Artificial Intelligence (AI) technologies, such as Reinforcement Learning (RL), automated configuration analysis, and Markov Logic Networks (MLNs), have shown great promise in automating, optimizing, and securing configuration management procedures. This will ultimately stop misconfigurations before they have a detrimental effect on system performance and dependability.

The use of MLNs in distributed system configuration management enables probabilistic reasoning, allowing systems to identify and fix misconfigurations based on dependencies between configuration parameters, as demonstrated by according to (1). This method improves the system's capacity for self-correction in dynamic contexts while lowering human error. Similar to this, the reinforcement learning techniques investigated by according to (2) highlight AI's capacity to dynamically modify system settings in response to observed behaviours, providing real-time adaptive solutions, particularly in systems that need constant configuration tuning.

Furthermore, as according to (4) showed in their study on stateful firewall misconfigurations, AI systems are essential for improving security. By detecting, evaluating, and resolving security vulnerabilities, AI-driven configuration management technologies help to maintain the strength of security rules and improve system defences against intrusions. These features are particularly important in next-generation networks and cloud settings, where AI-powered systems can adapt to configuration problems without the need for human intervention by implementing self-healing methods (according to (5)).

Even though AI has many advantages, there are still a number of obstacles to overcome, such as the high cost of processing, the requirement for vast amounts of high-quality data, and the difficulties in integrating it with current infrastructures. Additionally, especially in high-stakes situations, AI-driven solutions need constant supervision to make sure that automated choices match corporate objectives and legal requirements.
Further advancements in configuration management are anticipated as AI technologies advance. The expanding application of AI in edge computing and 5G networks, together with the creation of hybrid models that combine AI techniques like deep learning and reinforcement learning, will open up new possibilities for configuration management optimization in remote and extremely dynamic contexts. Additionally, maintaining openness and confidence in automated configuration procedures will depend on how well AI decision-making can be explained.

To sum up, AI-enhanced configuration management is an effective technique for enhancing security, reducing the likelihood of system misconfigurations, and increasing resilience. AI technologies will become

more and more important in managing intricate IT systems as they develop and mature, assisting businesses in preserving operational effectiveness, security, and dependability in a rapidly shifting technological environment.

7. Future Scope

The use of AI technologies in configuration management offers encouraging prospects for preventing system misconfigurations in settings that are becoming more dynamic and complicated as they develop. Thanks to developments in machine learning, reinforcement learning, and probabilistic reasoning, AI-enhanced configuration management has a wide range of potential applications in the future. In the upcoming years, AI can improve configuration management in the following important areas:

1. **System Self-Healing and Autonomous Setup**
   According to (6), the idea of self-healing has great promise for 5G networks and other applications. In the future, artificial intelligence (AI) systems may be able to recognize setup errors automatically and take immediate corrective action without human assistance. These self-healing capabilities will be applicable to cloud, edge, and hybrid computing systems, among other situations. AI may dynamically modify configurations depending on observed system states by utilizing reinforcement learning and Markov Logic Networks (MLNs), guaranteeing system resilience even in the event of a failure.

2. **Configuring Security and Enforcing Policies with AI**
   Maintaining safe and effective configurations is essential, especially in cloud settings and big dispersed systems. By continuously evaluating and modifying configurations to identify vulnerabilities, artificial intelligence (AI) can automate the execution of security policies (according to (5)). With further developments, AI systems will be able to identify security configuration errors as well as suggest and carry out preventative adjustments to stop possible intrusions or breaches. In dynamic contexts like the Internet of Things, cloud-native architectures, and 5G networks, this would be very pertinent.

3. **Optimization and Suggestions for Intelligent Configuration**
   According to (7), AI systems that actively suggest and carry out configuration modifications that maximize system performance will be a part of configuration management in the future. These systems will go beyond simply identifying misconfigurations. AI algorithms may recommend configuration changes to enhance scalability, lower latency, or boost fault tolerance by continuously observing network traffic, system load, and performance indicators. These artificial intelligence (AI) systems will provide customized solutions for intricate distributed architectures by learning from past data and adjusting to shifting environmental conditions.

4. **Configuration Management Trust and Explainable AI**
   Explainability and transparency of AI judgments will become crucial as AI-based systems assume greater responsibility for configuration management. Understanding how and why AI makes configuration decisions is essential for security-critical systems, such those described by according to (8), especially when those decisions have an impact on security policy. Explainable AI (XAI) approaches will be necessary for the future of AI-enhanced configuration management in order to provide insights into the decision-making process. This will enable human operators to verify the AI's activities and establish confidence in its suggestions.

5. **Federated Education for Dispersed Configuration Administration**
   The data needed to train AI models may be dispersed across several sites due to the growing usage of edge computing and IoT. Federated learning provides a scalable approach to distributed configuration management by allowing models to be trained locally and aggregated centrally without requiring data centralization. Federated learning is a perfect option for sectors like healthcare, banking, and telecommunications since it allows AI systems to learn from a variety of distributed systems and environments while protecting data privacy (according to (13).

8. References

[1] Schauer, R., & Joshi, A. (2016). Distributed system configuration management using Markov logic networks. *International Journal of Autonomic Computing*, *2*(2), 137-154.
[2] Bu, X., Rao, J., & Xu, C. Z. (2009, June). A reinforcement learning approach to online web systems auto-configuration. In *2009 29th IEEE International Conference on Distributed Computing Systems* (pp. 2-11). IEEE.
[3] Couch, Alva L. "System configuration management." In *Handbook of Network and System Administration*, pp. 75-133. Elsevier, 2008.
[4] Bu, X., Rao, J. and Xu, C.Z., 2009, June. A reinforcement learning approach to online web systems auto-configuration. In *2009 29th IEEE International Conference on Distributed Computing Systems* (pp. 2-11). IEEE.
[5] Garcia-Alfaro J, Cuppens F, Cuppens-Boulahia N, Martinez S, Cabot J. Management of stateful firewall misconfiguration. Computers & Security. 2013 Nov 1;39:64-85.
[6] Sánchez, José, et al. "Softwarized 5G networks resiliency with self-healing." *1st International Conference on 5G for Ubiquitous Connectivity*. IEEE, 2014.
[7] Li, F., Yang, J., Wu, J., Zheng, Z., Zhang, H. and Wang, X., 2014. Configuration analysis and recommendation: Case studies in IPv6 networks. *Computer Communications*, *53*, pp.37-51.
[8] Alfaro, Joaquin Garcia, Nora Boulahia-Cuppens, and Frédéric Cuppens. "Complete analysis of configuration rules to guarantee reliable network security policies." *International Journal of Information Security* 7, no. 2 (2008): 103-122.
[9] De Silva, Lakshitha, and Dharini Balasubramaniam. "Controlling software architecture erosion: A survey." *Journal of Systems and Software* 85, no. 1 (2012): 132-151.
[10] Alimi, R., Wang, Y. and Yang, Y.R., 2008, August. Shadow configuration as a network management primitive. In *Proceedings of the ACM SIGCOMM 2008 conference on Data communication* (pp. 111-122).
[11] Hershey, P. C., Rao, S., Silio, C. B., & Narayan, A. (2014). System of systems for quality-of-service observation and response in cloud computing environments. *IEEE Systems Journal*, *9*(1), 212-222.
[12] Singh, S., Jeong, Y.S. and Park, J.H., 2016. A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications*, *75*, pp.200-222.
[13] Al-Shaer, E. (2014). *Automated firewall analytics: Design, configuration and optimization*. Springer.
[14] Kang, E., & Jackson, D. A model-based framework for security configuration analysis. *Unpublished manuscript. Available at: http://people. sail. met. edu/eskang/papers/security-configuration. pdf*.
[15] Vecchiato, Daniel, and Eliane Martins. "Experience report: A field analysis of user-defined security configurations of android devices." *2015 IEEE 26th International Symposium on Software Reliability Engineering (ISSRE)*. IEEE, 2015.