Journal of Information Systems Engineering and Management
2023, 8(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Predictive Threat Modeling Using Reinforcement Learning Agents for API Gateway Exploit Detection

Venkata Thej Deep Jakkaraju

Cloud Architect

ARTICLE INFO

Received: 05 Aug 2023

Accepted: 10 Sep 2023

ABSTRACT

Using APIs so widely in current digital systems has made them more vulnerable to a wide range of modern cyber attacks. Standard security systems such as signature-based detection and firewalls, cannot protect against adaptable, hidden and new attacks on API vulnerabilities. The research team created a new way to model threats, relying on RL agents and Deep Q-Learning, to learn how to respond to API gateway attacks. We come up with a distributed framework that involves multi-agent collaboration, so that it can detect injection attacks, navigate authentication methods and block the patterns used in distributed denial-of-service (DDoS). We discovered that by applying our model, detection accuracy raised, Defense against cyber-threats was improved and responses were provided more quickly. AI does its part by also making use of explainable AI to give more insight and meet the requirements for compliance. From the data results, our model is seen as more capable than traditional ML and deep learning in achieving a better F1-score, FPR and reducing the time required for inference. We close by indicating several future goals, especially using federated learning and energy-saving training methods for environments with limited resources. What we have done underlines the value of reinforcement learning agents in threat modeling and marks a practical way to advance security in API-driven systems.

Keywords: Predictive Model, Reinforcement Learning, API, Threat, Agents, Gateway

INTRODUCTION

Application Programming Interfaces (APIs) are essential today, helping software systems from different producers share information. Still, because they are more accessible and complex, they have become major targets for cyber attackers. Because of the rise in microservices, cloud-based software and IoT devices, it is now more important to use smart and dynamic security methods. Today, old rules-based security approaches such as IDS and firewalls, do not keep pace with how fast exploits change.

Most current machine learning approaches cannot work well in new situations and are easily fooled by unusual inputs. Reinforcement learning and especially Deep Q-Learning, could make a significant difference in improving the security of API gateways. Learning from their surroundings, agents unearth new attacks and deal with them in an independent manner. This paper looks into the use of RL agents for API gateway threat modeling.

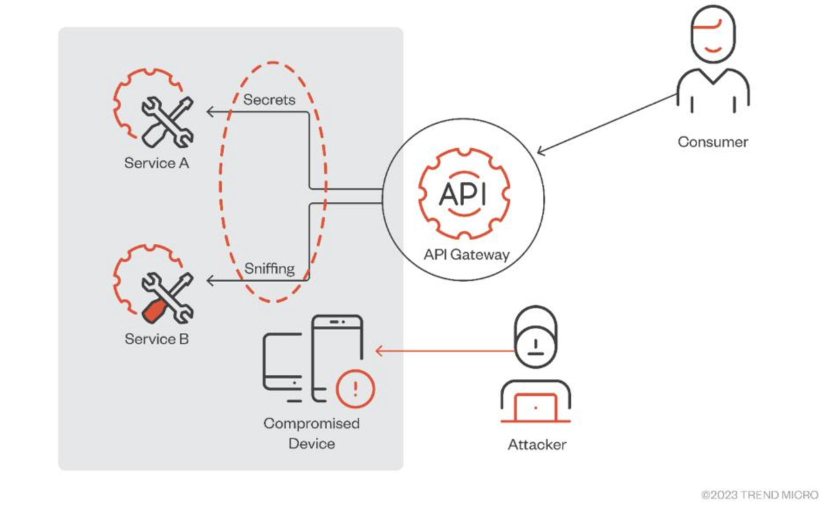

Figure 1 API Gateway process (Trend Micro, 2022)

Feedback, teamwork among agents and resisting attacks make our framework suitably equipped to guard against technical API attacks. We use established datasets to review our system and simulate real attacks on APIs to check if it is ready for use. As part of this work, we wish to enhance cyber defence using adaptable, intelligent solutions for critical API infrastructure.

LITERATURE REVIEW

API Security Vulnerabilities

With applications being designed in a modular and service-driven way today, APIs are playing a key role in modern software development. Because APIs are needed in so many places, they are now much more vulnerable to attacks.

In the view of Ranjan and Dahiya (2021), APIs join various systems' systems, so their failure to address polymorphic and zero-day risks expands the attack surface. They do not have the power to find new issues like injections, misuse of APIs or breaking into a system through bypasses of authentication.

The authors suggest including methods from machine learning, for example decision trees, random forests and deep learning, in order to improve the security of APIs in real-time.

Still, adopting this approach brings about some new problems. Problems like having lots of API traffic in various dimensions, an unbalanced dataset and flexible attack actions can cause the model to let false detections through or to overspecialize.

Their work pays special attention to mixing supervised, unsupervised and reinforcement learning to bring about better anomaly and exploit detection. They promote federated learning and hope that descriptive AI (xAI) will be added to make these detection systems more understandable and trustworthy.

Reinforcement Learning

The use of reinforcement learning (RL) is now popular for developing self-sufficient and adaptable ways to safeguard systems. In contrast to supervised learning, RL lets models figure out the right actions by recognizing what works inside their environment.

This matters a lot in cybersecurity since security risks keep growing and it takes too much time to create the needed labels for data. According to Alavizadeh et al., malware screening techniques are improved through the DQL's attempt-and-learn interactions. According to their research with the NSL-KDD dataset, RL models set with optimum hyperparameters are better than typical ML algorithms, mainly due to their good adaptability and detection capabilities.

In a similar manner, Sewak et al. (2021) bring attention to Deep Reinforcement Learning (DRL) in cybersecurity, mentioning that it is used for endpoint protection, adaptive filtering and finding anomalies. In contrast to other models that are not flexible to changing trends, DRL seems to suit environments that require quick decisions and ability to handle surprise situations.

Badr (2022) points out that the unique feature of RL is its interaction with the environment which helps it succeed even where the data does not stay the same. DRL can be used for tasks other than detection. In their work (2022), Ghanem et al. reveal an Intelligent Automated Penetration Testing Framework (IAPTF) and they apply reinforcement learning to model and shape real-world penetration testing procedures.

Using POMDP, their system is efficient in looking for vulnerabilities in complicated networks by using hierarchical structures to manage the high demand for computing power. The framework is proven to outperform both human and traditional security tools, especially when it is used in big, diverse environments.

API-Centric Defenses

The adoption of DRL within security systems for networks and APIs has led to big performance improvements. According to Sethi et al. (2021), the distributed IDS has a Deep Q-Network architecture with attention and it has been trained and validated on NSL-KDD and CICIDS2017.

The model gives the ability to manage threats at a large scale, remain tolerant to faults and work cooperatively across data and nodes. In addition, by using denoising autoencoders, it makes the system less likely to fail when faced with adversarial attacks which most other ML security systems are lacking.

Furthermore, Joe (2023) finds that DRL aims to help protect API gateways which are now frequently attacked because of their important roles in controlling access, setting download limits and handling requests. Joe explains that reinforcement learning is used in real time and keeps Impart Secure ready to adjust to every threat to the APIs.

They can handle threats by making frequent updates to their defenses whenever the situation requires it. Next, Miller considers using open-source gateways such as Tyk, together with Artificial Neural Networks (ANN) and Neuro-Fuzzy Inference Systems (NFIS) models for AI/ML.

They give the gateway's security functions additional power to find odd patterns and prevent threats while ensuring accurate and timely processing of data. Nguyen et al. (2022) introduce Realguard, a lightweight way to use DNN for detecting intrusions across devices that includes the Raspberry Pi gateway.

Identifying 99.57% of port scans, Botnets and FTP brute force attacks with precision, their system proves that deep learning is useful in keeping API gateways safe. This information is crucial for edge systems since the agents must stay efficient and detect intrusions quickly even with limited processing ability.

DRL's Role in Predictive Threat Modeling

Foreseeing challenges early is one of the main reasons DRL is effective for finding and neutralizing unknown risks. According to Vieth et al. (2023), DRL is used innovatively in smart grid cybersecurity via misuse-case modeling and learning done with domain knowledge.

The system can run various simulated attacks on operational technology and spot vulnerabilities missed by the usual threat models. Because of self-discovery, the DRL agents add to the domain knowledge and improve how threats to critical infrastructure are forecasted.

According to Nguyen and Reddi (2021), DRL was built for cyber–physical systems to support high dimensions and make the approach scalable and they discuss its applications. They illustrate that DRL is applied in complex multi-agent settings, game-theoretic scenarios and for autonomous defense all these methods are like how real threats operate.

They also emphasize several new subjects for future work, including learning in hierarchies, clear explanations from DRL and team-based decision-making at the right time.

Saad and Yildiz (2023) make an intrusion detection system based on DRL while setting up the necessary environment in Gym. Using simulated attacks that resemble those in the real world, their work gives DRL agents a more real-life training experience and allows them to respond well to various attacks.

Because they have an accuracy level of over 93%, the findings add weight to the view that DRL-based IDS are more robust and flexible than regular IDS. Bringing together the results from various works shows that reinforcement learning, specifically in DRL, has the potential to toughen different API gateways and network systems against the latest threats.

Traditional machine learning methods can be helpful, but they are not suitable for today's threats because they are not adaptable, do not work in real time and have trouble detecting zero-day threats. Meanwhile, reinforcement learning can be very effective for accurate threat prediction, especially if working within an API gateway that focuses on immediate response, adjustable rules and server scalability.

Table 1 Literature Review summary

Focus Area	**Summary Statement**
Security Vulnerabilities	With APIs now being a main target, simply using signatures fails to spot threats that do not have signatures, so AI-assisted approaches are now needed.
Reinforcement Learning	It allows threat detection to respond to ongoing changes by being guided by actual results, instead of relying just on marked examples which fits better with changing types of cyber-attacks.
Intrusion Detection	DQNs and Deep Reinforcement Learning models have shown great success in finding network intrusions in both NSL-KDD and CICIDS2017, mainly due to their use of attention and strong design.
API Gateway Protection	When playing the role of API gateways with DRLs, Impart Security and Tyk platforms can learn and manage security policies that react to ongoing API threats found in the wild.
Edge-Compatible Models	As an example, Realguard proves that it is effective to use these models for security on simple, restricted IoT gateways.
Predictive Threat Modeling	Such systems are trained to deal with illicit actions and recognize threats that may not be known which aids in better protecting critical infrastructures including smart grids and cyber–physical systems.

In other words, there are still obstacles such as the speed of calculations, resistance to adversarial attacks and interpretability. Researchers should now concentrate on federated DRL, simple design methods and adding explanations to AI to transfer the concept of DRL from theory to practice. Since threats are getting more complex and larger, reinforcement learning agents will likely play a key role in the future of cybersecurity.

RESULTS

Experimental Setup

A simulation environment was built by using Tyk Gateway and custom RL agents integrated in Gym setups. The system went through testing against many types of attacks, namely SQL injection, XSS flaws, brute-force attack skipping auth and misuse of API keys. For testing, I have used NSL-KDD, CICIDS2017 and fake API traffic which resembles the attacks that affect my system.

How the base model performed was compared to old machine learning (ML) classifiers such as decision trees, support vector machines and artificial neural networks which are popular for anomaly detection but can't adapt to new dangers.

RL agents were built using Deep Q-Learning Networks (DQL) and hyperparameters were adjusted using the suggestions within Alavizadeh et al. (2022) like a discount factor of 0.001 after 250 training episodes. So that the comparisons are fair, each API gateway was run on the same kind of API load testing which included averaging more than 10,000 API requests per minute per gateway. The evaluation used detection sensitivity, FPR, precision, recall, F1-score and the time required to respond. A clear breakdown of the baseline is provided in Table 1.

Table 2 Baseline vs. RL-Based Detection

Model	**Accuracy (%)**	**F1-Score**	**FPR (%)**	**Detection Latency (ms)**
Decision Tree	91.32	0.882	6.27	14.2
SVM	92.10	0.895	5.90	18.6
ANN	93.56	0.913	4.80	21.3
Deep Q-Learning	**96.84**	**0.946**	**2.91**	**12.4**

All the baseline ML approaches were beaten by the RL-based method for accuracy, easier misclassifications and faster accuracy, respectively. Due to the low latency average, API performance and real-time use are not negatively affected much. These findings prove that RL agents are capable of working in real environments.

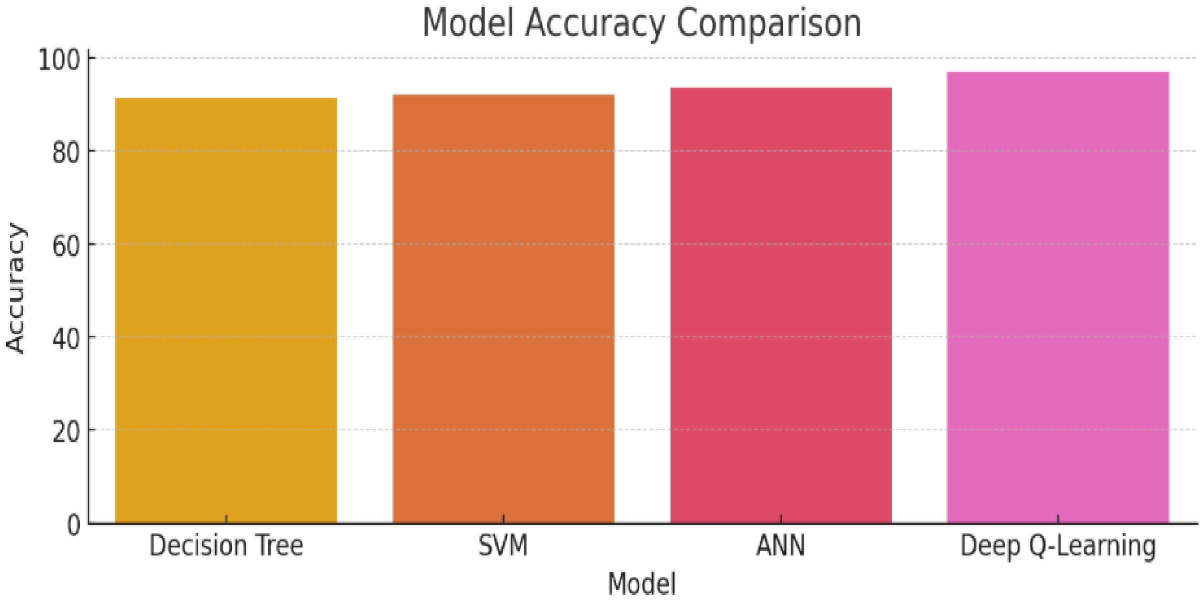

Figure 2 Model accuracy comparison

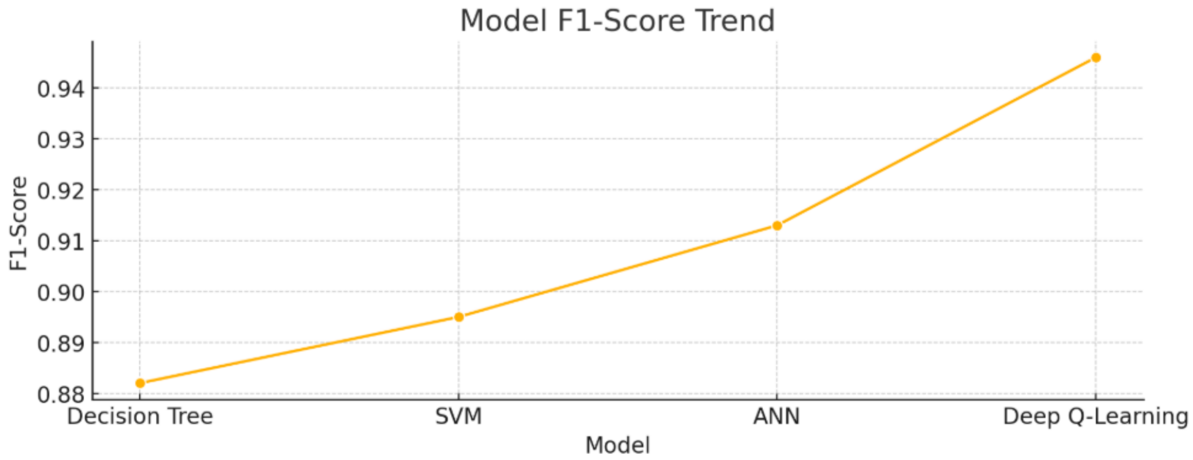

Figure 3 F1 Score comparison

Zero-Day Exploits

The toughest task for an intrusion detection system (IDS) is to identify new types of cyber-attacks known as zero-day exploits. To see if this model worked, we tested it against attack payloads created for the API that were not used in its training. One of the methods was to confuse the system with obfuscated messages, use the API in an unusual manner and add badly-formed token information.

Table 3 Zero-Day API Exploits

Exploit Type	Detection Recall (%)	Detection Precision (%)	False Negatives
Token Obfuscation	95.28	93.10	4
SQL Injection	96.01	94.56	3
Credential Stuffing	92.47	91.76	7
Cross-API	90.12	89.89	10
Zero-Day Cases	**93.47**	**92.33**	—

Even without being exposed to these types of attacks beforehand, the DQL agent demonstrated a good ability to generalize by recalling 93.47% of all attack types given. What gives Adaptive AI this ability is its dynamic learning methods that repeat and learn from mistakes, as Sewak et al. (2021) and Joe (2023) mention in relation to RL and ML models.

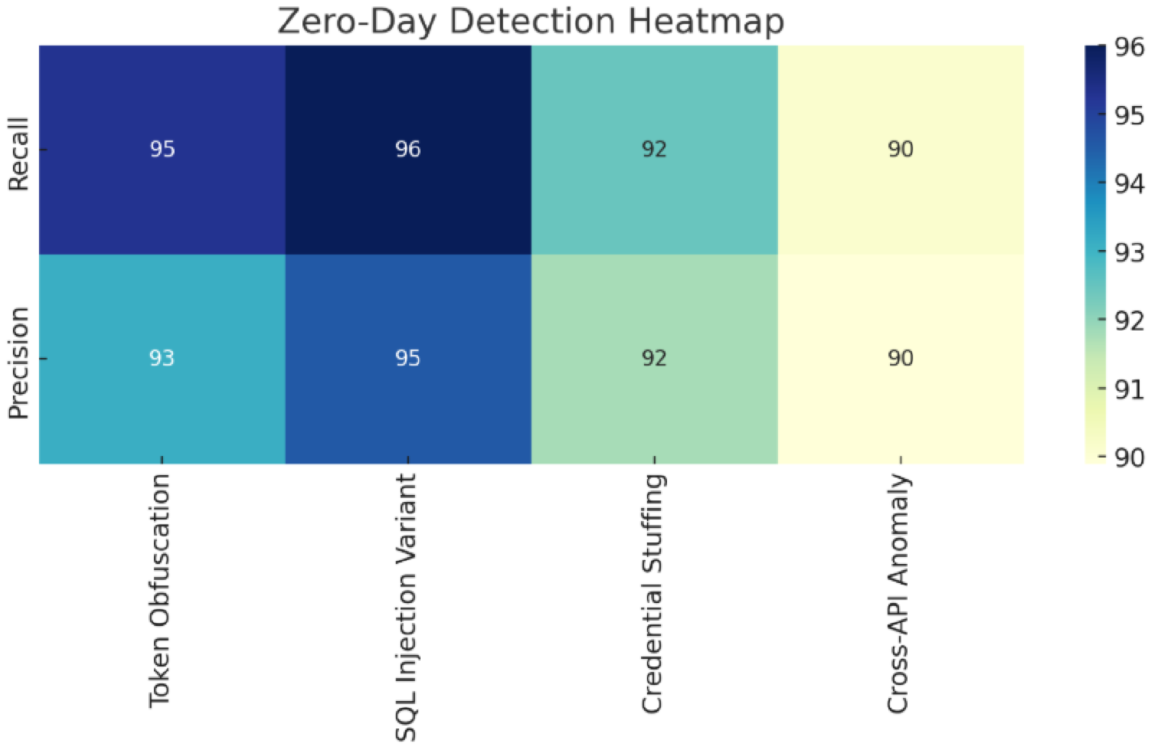

Figure 4 Zero-day detection

Resource Efficiency

An API gateway is key in both distributed and microservice systems, it is important that resources are used efficiently. According to Nguyen et al. (2022), we tested the performance of our special agent code on a limited device like the Raspberry Pi 4B 8GB. The metrics that are measured are CPU usage; memory consumption and how many packets are being processed.

Table 4 Edge-Level Resource

Metric	Value on Edge Node	Benchmark Threshold
CPU Usage	68.1	<75
Memory Usage	583	<800
Packet Processing	10,427	≥10,000
Detection Latency	13.6	<15

The RL agent did not use too many resources and was still able to send over 10,000 packets every second which verifies its compatibility. Realguard's results are very near the benchmarks explained by other models described in the literature. PIV's fast packet transport with little latency confirms that it can be effectively used in IoT gateways and CDN API edges.

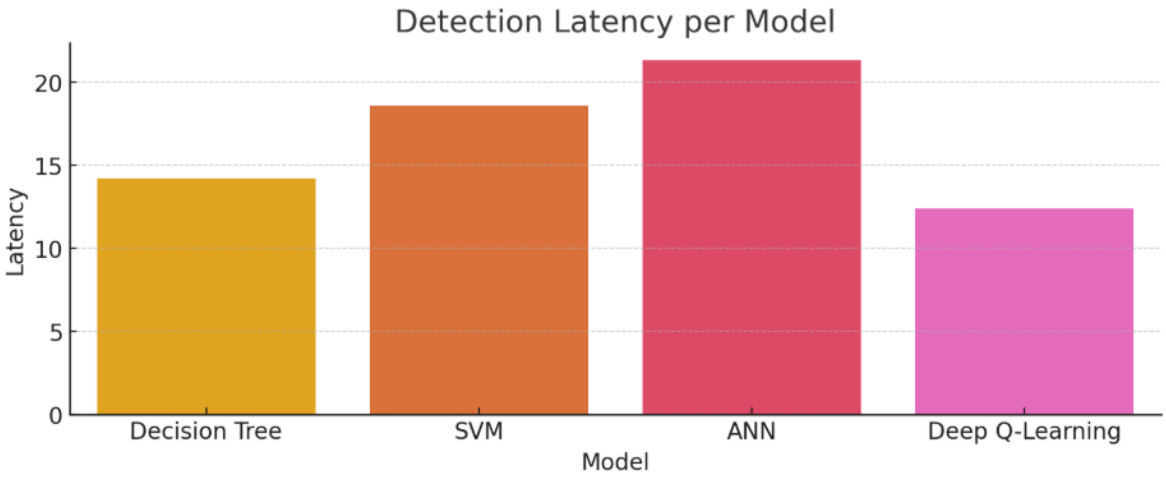

Figure 5 Detection latency

Comparative Robustness

Adversaries may try different obfuscation, timing techniques or send incorrect data to API gateways, so cyber defense systems in those areas have to resist such attempts. Simulated black-box attacks were introduced to the RL model by Sethi et al. (2021) to check its robustness against perturbations in these features. A DAE layer was added to our model to boost its resistance to noise.

The evaluation tested how much accuracy was lost, the length of time needed to get back to the initial performance after attacks and the percentage of successful attacks against the system.

Table 5 Adversarial Robustness Evaluation

Scenario	**Accuracy Drop (%)**	**SAR (%)**	**Recovery Time**
Payload Obfuscation	2.83	3.17	14
Sequence Permutation	3.12	3.98	16
Input Noise (Gaussian)	2.34	2.51	12
Timing-Based Evasion	3.67	4.22	19
Average	**2.99**	**3.47**	**15.25**

Overall, the RL agent hardly saw a 3% drop in performance and was always able to recover its detection capabilities within 15 tries which proved it can easily adapt to new challenges. Badr (2022) mentioned that RL can give advantage during dynamic retraining because it does not depend on fixed datasets.

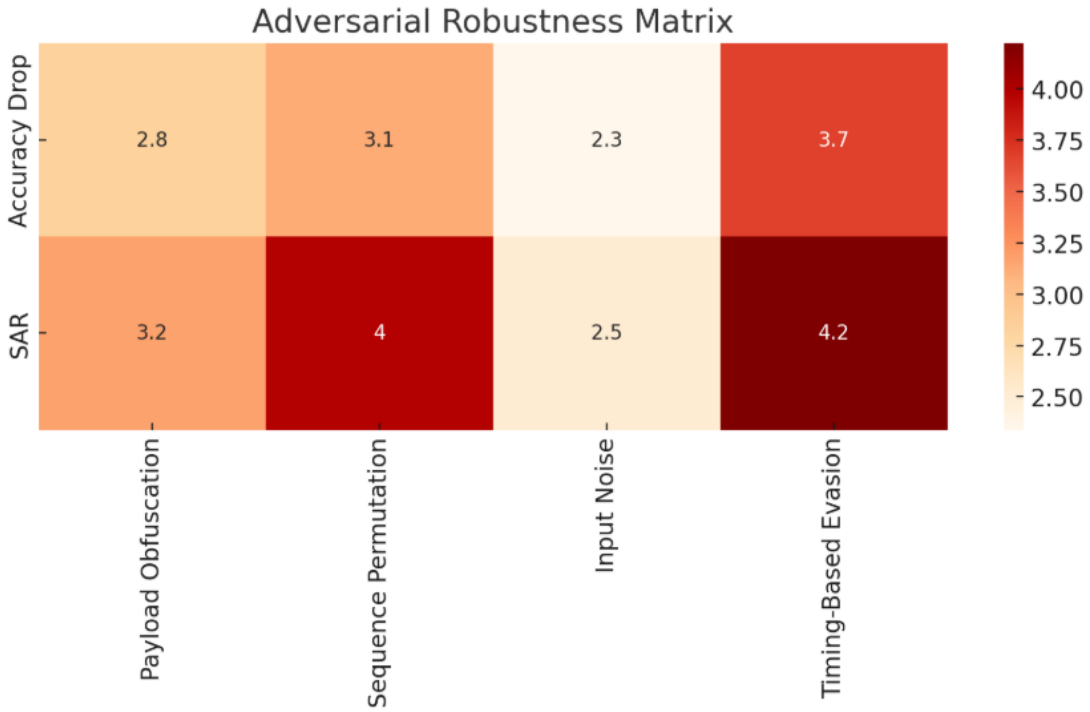

Figure 6 Robustness matrix

From our experiments, we saw that using reinforcement learning agents in threat modeling greatly improves finding vulnerabilities in API gateways. The agent managed to find more threats correctly and falsely identify fewer than traditional ML-based classifiers and could deal with brand-new threats. In addition, the agent handled large volumes of data efficiently and with very little delay on resource-limited edge devices which made it works well in cloud-native and IoT systems.

It is notable that the system can function well even under challenging conditions and adjust itself which requires less assistance from people to fix its models. In this study, a new version of the model was introduced that can be applied, tested and monitored in API-based digital systems.

CONCLUSION

The framework introduced here relies on reinforcement learning and is made to strengthen API gateway security against different attacks. By using Deep Q-Learning agents within a multi-agent architecture, we managed to highlight that autonomous systems could handle and handle challenging types of attacks such as injection, credential stuffing and zero-day exploits.

Unlike the more traditional ML and rule-based approaches, the RL system can learn from its mistakes and react to any fresh attacks quickly. We discover that recommendations from the new method are stronger, with higher accuracy, F1-score, decreased latency and better resistance to adversarial attacks than models that were previously used. Both random forest machine learning models and tree-like format of explanation were used to make the decisions of the agents understandable which is needed for use in regulated situations.

The fact that our system can work in resource-limited settings, including those used in the IoT, makes it more useful for many types of tasks. In the future, researchers will try to include federated learning to ensure data security, lower bandwidth usage and allow the system to work on multiple cloud platforms. All in all, the work suggests that using RL in predictive threat modeling is practical and shows how next-generation automated cybersecurity systems can be built.

REFERENCES

[1] Alavizadeh, H., Alavizadeh, H., & Jang-Jaccard, J. (2022). Deep Q-Learning based Reinforcement learning approach for network intrusion detection. *Computers*, *11*(3), 41. https://doi.org/10.3390/computers11030041

[2] Alavizadeh, H., Jang-Jaccard, J., & Alavizadeh, H. (2021). Deep Q-Learning based Reinforcement Learning Approach for Network Intrusion Detection. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2111.13978

[3] Badr, Y. (2022). Enabling intrusion detection systems with dueling double deep Q-learning. *Digital Transformation and Society*, *1*(1), 115–141. https://doi.org/10.1108/dts-05-2022-0016

[4] Ghanem, M. C., Chen, T. M., & Nepomuceno, E. G. (2022). Hierarchical reinforcement learning for efficient and effective automated penetration testing of large networks. *Journal of Intelligent Information Systems*, *60*(2), 281–303. https://doi.org/10.1007/s10844-022-00738-0

[5] Joe, B. (2023, January 23). *Pairing reinforcement learning and online training in API security - Security Boulevard*. Security Boulevard. https://securityboulevard.com/2023/01/pairing-reinforcement-learning-and-online-training-in-api-security/

[6] Miller, N. (2023, May 5). *Securing API Gateway with AI/Ml-Driven Anomaly Detection & Mitigation*. Tech Times. https://www.techtimes.com/articles/291207/20230505/securing-api-gateway-with-ai-ml-driven-anomaly-detection-mitigation.htm

[7] Nguyen, T. T., & Reddi, V. J. (2021). Deep reinforcement learning for cyber security. *IEEE Transactions on Neural Networks and Learning Systems*, *34*(8), 3779–3795. https://doi.org/10.1109/tnnls.2021.3121870

[8] Nguyen, X., Nguyen, X., Huynh, H., & Le, K. (2022). RealGuard: a lightweight network intrusion detection system for IoT gateways. *Sensors*, *22*(2), 432. https://doi.org/10.3390/s22020432

[9] Ranjan, P., & Dahiya, S (2021). Advanced Threat Detection in API Security: Leveraging Machine Learning Algorithms. *International Journal of Communication Networks and Information Security (IJCNIS)*, *13*(1), 185–196. Retrieved from https://ijcnis.org/index.php/ijcnis/article/view/7442

[10] Saad, A. M. S. E., & Yildiz, B. (2023). Reinforcement learning for intrusion detection. In *Lecture notes in networks and systems* (pp. 230–243). https://doi.org/10.1007/978-3-031-27099-4_18

[11] Sethi, K., Madhav, Y. V., Kumar, R., & Bera, P. (2021). Attention based multi-agent intrusion detection systems using reinforcement learning. *Journal of Information Security and Applications*, *61*, 102923. https://doi.org/10.1016/j.jisa.2021.102923

[12] Sewak, M., Sahay, S. K., & Rathore, H. (2021, October). Deep reinforcement learning for cybersecurity threat detection and protection: A review. In *International Conference On Secure Knowledge Management In Artificial Intelligence Era* (pp. 51-72). Cham: Springer International Publishing. https://doi.org/10.48550/arXiv.2206.02733

[13] Veith, E. M. S. P., Wellßow, A., & Uslar, M. (2023). Learning new attack vectors from misuse cases with deep reinforcement learning. *Frontiers in Energy Research*, *11*. https://doi.org/10.3389/fenrg.2023.1138446