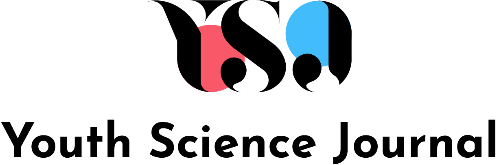
Computer Science



Ultimate security by the combination of Cloudflare’s and Akamai’s APIs and machine learning.

Abdelrahman Abdelwahab, STEM high school for boys- 6th of October.

Ahmed Osama, WE for applied technology.

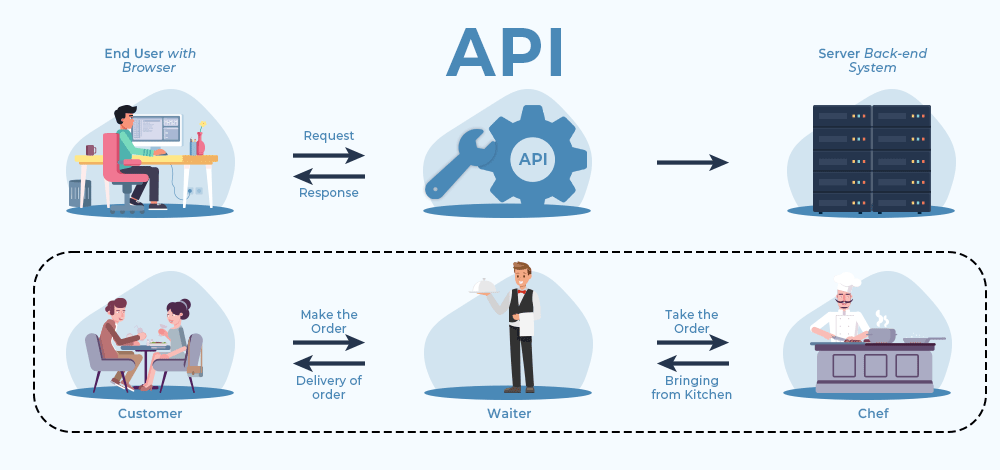
Abstract

*Write down here your abstract. The abstract should be a brief summary of the research article on this particular subject and should easily help the reader know the article’s main scope and purpose. The abstract should not be less than 50 words or more than 250.*

1. **Introduction**

Due to the existence of the great growth in technologies, the need to implement a secured network is increasing [1]. The gross usage of computerized systems has raised critical threats with hacking [1].

Hacking is a way to find the weak points of a system or network and use these points to access, edit, or gain data without legal authentication. Instead, the hackers may break down the system [2]. By 2025, cybercrime will cost the world $10.5 trillion yearly [3]. This amount is greater than the half Gross Domestic Product of Europe. In 2023, 30,000 websites are hacked daily, and 64% of companies worldwide have experienced at least one form of cyber-attack [3].

Cloudflare’s API is enormous servers that increases security and reliability. “It does that by serving as a reverse proxy for the user web traffic” [3]. Also, Akamai does the same. Unfortunately, both have been hacked.

Therefore, the implementation of a new security system comes. This paper discusses the implementation of a security system made from the combination of Cloudflare’s and Akamai’s APIs and ML- to detect whether the IP is safe or suspicious. It first explains Cloudflare’s and Akamai’s APIs. Second, the ML model. Third the result from the combination of all.

Figure (1) illustrates the mechanism of API.

1. **Explanation of used tools**

API (Application Programming Interface): An API, or Application Programming Interface, is a set of rules and protocols that allows different software applications to communicate and interact with each other as Figure (1) illustrates. It defines the methods and data structures that developers can use to build and integrate various software components without needing to understand the inner workings of each component. APIs enable developers to leverage the functionality of other software systems, services, or platforms, making it easier to create complex applications by using pre-built building blocks. [7]

APIs play a critical role in modern software development by enabling developers to access services, retrieve data, perform actions, and integrate with external systems seamlessly. They can be used for various purposes, such as retrieving data from databases, interacting with web services, controlling hardware devices, and more. APIs can be designed for different levels of abstraction, from low-level system APIs that interact with hardware components to high-level APIs that provide specific functionalities like payment processing, social media integration, or cloud services. [7]

Diagram of a cloud network

Description automatically generatedCloudflare is a CDN and internet security company that offers services such as content delivery, DDoS protection, security enhancements, and optimization tools. It operates by routing website traffic through its globally distributed network of servers as Figure (2) shows [8].

Figure (2) demonstrates the mechanism of Cloudflare.

DNS Configuration: Update your domain's DNS records to point to Cloudflare's DNS servers. Cloudflare will then manage your domain's traffic.

Content Delivery: Leverage Cloudflare's content delivery network to cache and serve static assets from their edge servers, reducing load times and server loads.

Security: Enable Cloudflare's security features such as Web Application Firewall (WAF) to protect against attacks like SQL injection and cross-site scripting.

A diagram of a cloud network

Description automatically generatedLoad Balancing: Use Cloudflare's load balancing capabilities to distribute traffic across multiple servers for better performance and availability [8] as Figure (4) shows.

Figure (4) illustrates how Cloudflare balances the load.

Akamai is another major CDN provider with a focus on content delivery, application acceleration, and security [9].

Edge Server Configuration: Configure Akamai's edge servers to cache and serve content. Akamai's global network helps deliver content quickly to users around the world [9].

Performance Optimization: Utilize Akamai's performance optimization features to compress and optimize assets, reducing load times and improving user experience [9].

Application Acceleration: Leverage Akamai's acceleration technologies to enhance the performance of web applications and APIs [9].

Security Solutions: Akamai offers security solutions like DDoS mitigation and bot protection. Integrate these solutions to enhance security alongside Cloudflare's offerings. [9] as Figure (6) shows.

A diagram of a cloud with text and symbols

Description automatically generated

Figure (6) provides what Akamai’s API protect.

1. **Methods**

Combining Akamai, Cloudflare, and AI can create a powerful solution that enhances the performance, security, and intelligence of your web applications:

1 - Assessment: To create this new complex security we need to understand our network - application needs, traffic patterns, and potential AI Cases.

2 - Solution Selection: The areas in which machine learning can provide value need to be identified such as real-time threat detection. [4]

3 - Data Collection And Preparation: In using machine learning technology by giving some data "blocked data - safe data" - so the AI detects the blocked data and prevents it from accessing the application or the network also the AI will predict if the blocked data changed or got a new shape.[5] In that case, those data were gathered to check Internet protocols instead of predicting them [6]. The dataset of suspicious and safe IPs was collected (qualitative data). The number of IPs is greater than 30 thousand. The data is analyzed and divided into two categories safe and suspicious. Then, a logistic regression model- a type of ML- was implemented. The model trained on that data.

4 - Integration Between Akamai API and Cloudflare API: Integrate Cloudflare, Akamai, and machine learning. will involve leveraging APIS " AKAMAI API - CLOUDFLARE API ". and hooks provided by these platforms to incorporate AI-driven decisions.

5 - Security Enhancement: Leverage both Cloudflare and Akamai security features to create a multi-layered security approach. Implement Distributed Denial-of-Service Attack " DDoS " mitigation, bot protection, and OWASP " The OWASP Foundation " top 10 security measures through both platforms.

6 - Monitoring and Analytics: Using both Akamai and Cloudflare's monitoring tools to gain insights into applications - networks performance, user behavior, and security threats.

Integrate analytics tools to track user engagement, conversion rates, and other relevant metrics.

7 - Redundancy: Configuring failover mechanisms using both Akamai and Cloudflare's load balancing and traffic management features. Ensure that if one service experiences downtime, traffic seamlessly shifts to the other without major disruptions.

8 - Optimization: Continuously refine your AI models based on feedback and performance data. Iterate on your strategies to achieve better results over time.

1. **Section Heading**

If you want to divide your section into even more parts, then you can use this style for it. Remember, this is **optional**. Like this:

1. Example Sub-Section Heading

Then, you can add as many sub-sections as you would like using this style to your article.

1. Example Sub-Section Heading

You can add as many of these sections as you want and label them as you want. These sections will act as your **main body** of the article, where you can discuss the main topics. For example, you could have a section describing a certain researcher’s findings, biological mechanisms or phenomena. Make sure to use **in-text citations** and a lot of references to your claims.

1. Example Sub-Section Heading

You can add as many of these sections as you want and label them as you want. These sections will act as your **main body** of the article, where you can discuss the main topics. For example, you could have a section describing a certain researcher’s findings, biological mechanisms or phenomena. Make sure to use **in-text citations** and a lot of references to your claims.

1. Example Sub-Section Heading

You can add as many of these sections as you want and label them as you want. These sections will act as your **main body** of the article, where you can discuss the main topics. For example, you could have a section describing a certain researcher’s findings, biological mechanisms or phenomena. Make sure to use **in-text citations** and a lot of references to your claims.

1. **Conclusion**

This is the last part of the main body of the review article. Here, you’d summarize all the topics brought up in this review article like the abstract, but also conclude all the topics that was mentioned throughout the whole articles in this section.

1. **References**
2. R. Nair, C. P. Kasula, S. Vankayala, and N. Chakraborty, “IP network anomaly detection using machine learning,” *2019 IEEE 5th International Conference for Convergence in Technology (I2CT)*, 2019. doi:10.1109/i2ct45611.2019.9033545
3. A. Gupta and A. Anand, “Ethical hacking and hacking attacks,” *International Journal Of Engineering And Computer Science*, 2017. doi:10.18535/ijecs/v6i4.42
4. R. Vardhman, “How many cyber attacks happen per day in 2023?,” Techjury, https://techjury.net/blog/how-many-cyber-attacks-per-day/#:~:text=Globally%2C%2030%2C000%20websites%20are%20hacked,ransomware%20cases%20grew%20by%2092.7%25. (accessed Aug. 22, 2023).
5. E. Nygren, R. K. Sitaraman, and J. Wein, “Networked Systems Research at akamai,” ACM SIGOPS Operating Systems Review, vol. 44, no. 3, pp. 1–1, 2010. doi:10.1145/1842733.1842735
6. S. K. Jauhar et al., “How to use no-code artificial intelligence to predict and minimize the inventory distortions for Resilient Supply Chains,” International Journal of Production Research, pp. 1–25, 2023. doi:10.1080/00207543.2023.2166139
7. stamparm, “Blocked data,” github, 2023.
8. J. Ofoeda, R. Boateng, and J. Effah, “Application programming interface (API) research,” International Journal of Enterprise Information Systems, vol. 15, no. 3, pp. 76–95, 2019. doi:10.4018/ijeis.2019070105
9. M. Nadeem et al., “Preventing cloud network from spamming attacks using Cloudflare and KNN,” Computers, Materials &amp;amp; Continua, vol. 74, no. 2, pp. 2641–2659, 2023. doi:10.32604/cmc.2023.028796
10. E. Nygren, R. K. Sitaraman, and J. Wein, “Networked Systems Research at akamai,” ACM SIGOPS Operating Systems Review, vol. 44, no. 3, pp. 1–1, 2010. doi:10.1145/1842733.1842735