International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 07 | July 2022 www.irjet.net p-ISSN: 2395-0072

Webhook Support for Alert Policies

[1] K Anjani Vaibhavi, [2] Anala M R

[1,2] Department of Information Science and Engineering, R V College of Engineering, Bangalore, India

---

Abstract - *Corporate employees have numerous duties, and yet no matter how many activities they must complete on a daily basis, confidentiality and reliability is usually always the top priority. Assurance that one's system and its assets are secure from public and cybersecurity hazards is essential in the business world — and as a result, the capacity to offer real-time notifications to customers may seriously affect any firm. One must act quickly to halt a continuing event before it causes permanent damage to your networks and resources. Alerts are a medium of communication between a system and its user. Alerting allows individuals to stay up to date on the information that is important to them. An alert system that is efficient, secure, and dependable lowers the cost of exchanging goods and services.*

Key Words: ***Webhook, alerts, Reactjs, graphql, webhook testing***

1.INTRODUCTION

In the field of cyber security, alert notifications are amongst the most significant data resources. These alert and tell your Technology staff regarding the current hacking attacks, suspicious activities, and every other issue that may endanger your firm and which is why alerts are vital for the firm's safety. Alert system contains notifications that notify customers of critical security issues or dangers to one's device or intranet. It is critical for a company's security personnel to intervene swiftly in numerous security situations and manage any dangers while these pose major difficulties.

1.1 Alert Notification Systems

Alerts are messages that warn you of severe security concerns or risks to any device or software. It is critical for the IT personnel to respond promptly in different security related events and control any dangers before they trigger major difficulties.

An alert notification service's principal role or goal is to swiftly warn personnel of possible dangers or exceptional circumstances and to offer guidance about how to react to such concerns. It is essential that any firm should follow these alerts or concerns and warn the customers to achieve a reliable and safe network and devices.

1.2 Webhooks

Webhooks are notifications that are sent automatically by applications when any problem occurs. They contain content, or payload, and are delivered to a custom Domain, which is effectively the app's contact information or email. Webhooks are usually quicker and involve minimal effort on the user side.

Applications and organizations can use webhooks to transmit automatic messages and data to different services. These are an effective way for any system to communicate with one another and be automatically alerted when anything important occurs. Webhooks allow users to send content through one application to another seamlessly.

The objective behind this work is to integrate the alert notifications with webhooks for the user to automatically receive messages in case of any issues or security breaches and the benefits of the following integration. A method to integrate the alert notification system and the webhooks is shown

2. RELATED WORKS

The subject of alert notifications and webhooks is a modern way of warning the users about the critical issues. In this section, several relevant and well-known papers are studied to understand what the present systems offer and how they operate.

The author of [1] describes several effective techniques for addressing similar issues inside the project, hence improving the efficiency of the ReactJS App in a chain of processes. It also presents a time-efficient research approach for finding items in a huge data collection. In [2] the authors paper provided a method for monitoring the implementation of communal acts on Fb as well as the performance of corporate duties. Combining activities like posting and commenting progress in the development of social streams. Webhooks are used to "watch" to updates that occur on Facebook profiles.

Various GraphQL query processing algorithms are assessed and their efficacy was evaluated while handling only with N+1 issue in [3]. [4] explains a modular approach which could present customers' PHR quickly combining GraphQL and React Native, and therefore how utilising graphql in a clinical diagnostics may enable api calls faster, simpler, and more economic. The authors introduce in [5], how an

artificially intelligent agent may do this work rather than people directly accessing the internet and provide data as if the webpage had deployed an useability. They discussed the specifics and merits of this structure.

In [6], the author suggested a method has avoided the need of costly monitoring devices as feed and alert system ways. It has been able to discern movements and snap photos, and also send Alert messages through GSM along with e-mail notifications linked to the picture or file. In[7], the authors discussed about how the alert notification service benefits the users or clients in getting the required information from the services.

The proposed alert notification system integrates alert policies by sending warning messages by following methods like emails or webhooks.

3. BENEFITS OF ALERT NOTIFICATION SYSTEM

A. Customizable messages

Webhooks are integrated with a payload which allows the user to customize the content of the notification that is sent to the domain address. This lets the user to send the appropriate message according to the alert policy and type.

B. Computerized Alerting and responses

If a problem is ignored, the warning system immediately alerts the appropriate staff members or selected people based on a specified on-call schedule or the stated webhook, and escalates to higher standards of protection.

C. Simple Incorporation

Because modern IT infrastructures are so complicated, it's critical to choose a service that is simple to self-serve and interact with. This furthermore enhances the ROI of existing and emerging IT expenditures by allowing information to be shared more effectively between platforms and remote personnel.

D. Monitoring and Accounting

Alert and issue monitoring, auditing, and monitoring are critical tools for assisting groups in determining from which one can improve performance and effectiveness by optimizing response procedures, fine-tuning incident triggers and notifying, and perhaps more.

E. High Availability and Reliability

Since dependable monitoring is so vital, it's essential to engage in a platform that has organization structural resilience or scalability to avoid exposing the organization to hazards. An alerting system should be available and comply with tight Service level agreements, thus it is critical to choose a provider that is open around its backup and does not have planned service periods.

4. METHODOLOGY

An alert notification system should inform on all sorts of warnings and issues that happened in one's system related to unit procurement, setup, and data access. Consumers get the choice of sending an email to the relevant team personnel or using Webhooks as a transportation mechanism whenever these prompts occur when establishing these Alerts & Occurrences. This may be incredibly valuable for developing efficient event-driven processes, interacting with some other 3rd party apps, or troubleshooting the systems and intranet.

In the proposed system the alert notification system contains different alert policies. Each alert policy can be categorized by their type and is integrated with two options - a) Sending email to admins or appropriate team personnel b) Notifying via webhooks. These alert policies help the users to know any critical issues occured. Fig 1 shows the basic architecture of the alert notification system.

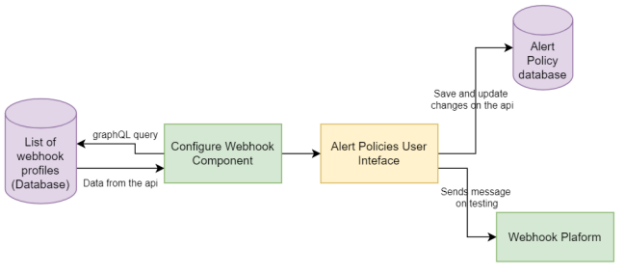

Fig-1 : Architecture of alert notification system

a) Webhook Structure

Each webhook is associated with a url and a payload. Payload contains the information about it. In general it can contain wbhook_body, webhook_id, webhook_headers and other information describing the webhook.

b) Email Administrators / Personnel

An email can be sent to the required or selected administrators/ personnel using customised HTML emails when an alert is triggered.

c) Using Webhooks

Whenever a Warning is set to send as a Webhook notification to the client, the notification is sent as a JSON formatted text using a POST request. The returned object has multiple fields , that JSON object provides data on the policy involved, the severity of the warning, and other facts and attributes.

d) Test the webhook profile

On clicking the test button after selecting the webhook, the 'text' part of the body entered is sent to the platform chosen as a notification/message.

e) Save Changes

After the entire process, the user is given an option of saving the changes he made, on clicking this, the changes are made and saved into the api. These changes reflect when the page is again opened for further use.

f) Alert policy fields

Every alert policy can contain a special field like webhook_profile_id and webhook_profile_payload integrated with the certain alert policy. Every time an alert occurs the warning is sent to that particular webhook url using the webhook_id associated with it and also payload with it is sent as the body of the content. This alert policy can be modified to select a particular webhook from the available ones and the content can be changed and saved.

Integration of ReactJS, graphQL and nodeJS makes the system more efficient. GraphQl can make queries to only get the required information from the api, rather than everything. Figure 2 shows the flowchart of an alert notification system.

5. RESULTS AND ANALYSIS

The alert notification system provides an easy and efficient to communicate with clients or personnel regarding critical issues in the system. The options of notify webhook and email admin(s)/notify webhook can be added to the alert policy.

The available webhook profiles are listed in a dropdown for the user to select and also an option to create a new profile can be given. The selected webhook profile displays the details of it such as method, url, headers and body.

The webhook body is made editable for user to send the required payload and validate it. A new field $format_alert_msg can be added to the webhook to get the customized payload which includes the data about the alert policy.

The webhook will be tested by sending the details to the api and a status code and message is received and shown to the user. Save changes button is added to the policy to save all the changes made to the policy like the webhook profile id and payload to customise it.

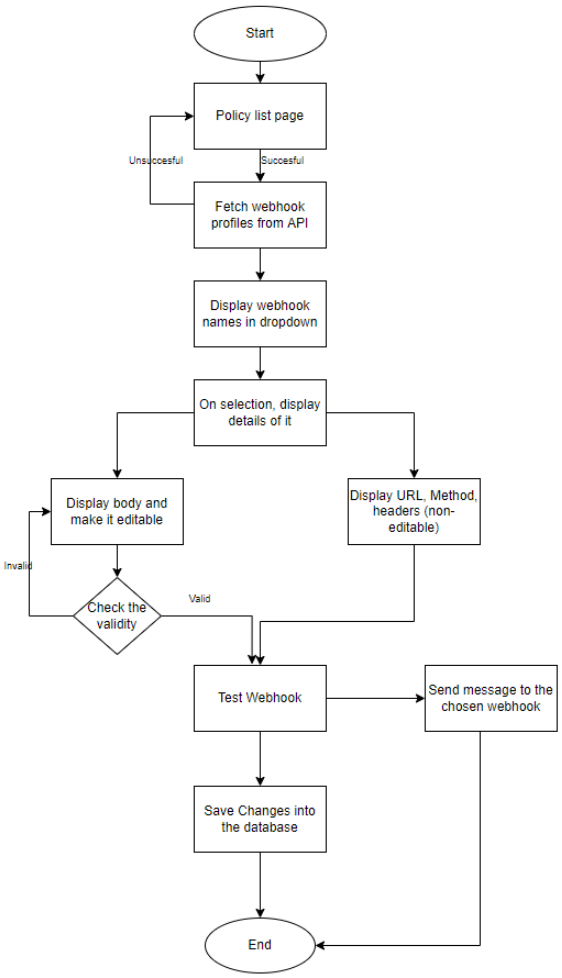

Fig-2 : Flowchart of alert notification system

6. DRAWBACKS OF ALERT NOTIFICATION SYSTEM

An alerting system is designed to transmit messages to a large group of people as rapidly and feasible. But it does come with its drawbacks. Some of them include -

Software glitches - Certain events might be so disastrous that all control systems collapse, rendering a warning scenario useless.

Without maintaining personal information up to date - A notification chain is as strong like its address book. When you aren't capable of reaching the individuals you need to reach, if you don't maintain email contact information updated. It is impossible to contact them.

Costly - Certain emergency alert solutions in this industry are significantly much costly over others. This might not be rational decisions options based on the industry's revenue and expenditure status.

Indifference - If receivers weren't taught to comprehend why and how the warnings are really issued and the reason they should get to respond, sometimes the personnel may not hold them accountable adequately.

7. CONCLUSION AND FUTURE SCOPE

An alert notification system with the support of webhooks is proposed which is based on sending alert messages to clients by using emails or webhooks.

To summarize publishing the Alert events to a Webhook listener is a most preferred & adoptable way for these enterprise customers to automate the flow from Incident detection to closure. This project gives a user friendly interface to the customers to interact with the system and makes the work easier. This feature will let the user send the alert body to the webhook profile selected. It also gives the option for the user to customise their message by adding a new field $format_alert_msg. It shows the response from the webhook on the interface.

The proposed system can include some features where webhook profiles can be categorised according to the type of the alert policy. Webhooks can also be restricted to have all the required data with correct information.

The save changes should work even if there is no modification in the condition if there is a change in the details of the webhook. Validation of the body needs to be done to prevent incorrect messages.

A feature to minimise the alert noise and filter spam can be added using machine learning models. Further enhancements can include the auditing and reporting of the issues and dynamic warnings can be sent to the client.

REFERENCES

[1] Arshad Javeed "Performance Optimization Techniques for ReactJS," in 2019 IEEE International Conference on Electrical, Computer and Communication Technologies

[2] Emir Ugljanin; Noura Faci; Mohamed Sellami; Zakaria Maamar," in 2020 IEEE International Conference on Enabling Technologies:

[3] Piotr Roksela; Marek Konieczny; Slawomir Zielinski, "Evaluating execution strategies of GraphQL queries," in 43rd International Conference on Telecommunications and Signal Processing (TSP) 2021

[4] Dong-cheol Jeon; LIUHAOYANG; Heejoung Hwang, "Design of Hybrid Application Based on GraphQL for Efficient Query for PHR“ in International Conference on Information and Communication Technology Convergence (ICTC) 2019

[5] Marjan Gusev; Sasko Ristov; Goran Velkoski; Pano Gushev, “Alert notification as a service” in International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) 2020

[6] Zazilah Binti May; “Real-time alert system for home surveillance”, in IEEE International Conference on Control System, Computing and Engineering 2019.

[7] Marjan Gusev; Sasko Ristov; Goran Velkoski; Pano Gushev, “Alert notification as a service”, in 43rd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) 2020.