MAAS- Monitoring as a Service through Payment Gateway

Vishvajit Jadhav[1], Ishwar Khedkar[2], Aniket Bobade[3], Atharv Kulkarni[4], Navnath Bagal[5]
Computer Department, Savitribai Phule Pune University

Abstract: This paper describes the creation of a cloud-based Monitoring as a Service (MaaS) platform designed specifically for thorough and safe payment gateway monitoring. Scalability, strong security, and real-time transaction insights are provided by the MaaS project through the use of the ELK Stack (Elasticsearch, Logstash, Kibana). Flexibility in monitoring modules allows for the smooth integration of the ELK Stack for effective analysis and display of vital payment gateway data. An interface that is easy to use enables operators to keep an eye on transactions and spot possible problems. Further integration with internal security and fraud detection tools is made easier by thoroughly described APIs. The goal of this MaaS platform is to improve oversight capabilities for crucial payment gateway operations by providing a consolidated, secure monitoring solution. Future development will involve adding machine learning for anomaly detection and extending data source support to cover other payment channels.

I. INTRODUCTION

Cloud-based payment gateways, the lifeblood of the digital world, beat with an ever-increasing complexity. A revolution in monitoring is necessary to protect these vital systems and guarantee smooth transactions. This paper introduces a novel solution: a customized Monitoring as a Service (MaaS) platform designed especially for the safe and thorough supervision of payment gateway operations. Imagine receiving real-time transaction insights with the ELK Stack's (Elasticsearch, Logstash, Kibana) capability. This MaaS project, which provides unmatched scalability and strong security, unleashes that very promise. Flexible monitoring modules take on the role of watchful guardians, gathering vital payment gateway information. This data easily connects with the ELK Stack, enabling effective analysis and intuitive visualizations to turn it into actionable intelligence. Operators are able to see transactions from above, which gives them the ability to spot possible problems early on and take appropriate action. Additionally, properly defined APIs serve as links, encouraging additional integration with current fraud and security detection systems.

This MaaS platform is a protector of the financial ecosystem, not merely a monitoring tool. It secures and centralizes oversight, giving operators the ability to guarantee the orderly flow of business and safeguard private financial information. Even more opportunities are ahead: using machine learning to detect fraud proactively, extending data source support to cover a broader range of payment methods, and enabling deeper transaction analysis with sophisticated visualization tools. With the help of this MaaS project, payment gateway monitoring enters a new era that is secure, scalable, and allows for total transaction oversight.

II. LITERATURE SURVEY

1) FEDARGOS- V1: A Monitoring Architecture for Federated Cloud Computing Infrastructures , IEEE Access (Vol. 10) , 2022. FEDARGOS-V1 offers a new architecture for monitoring federated clouds, improving throughput but potentially lacking scalability compared to DRAGONS. For our ELK-based project, prioritize scalability, data flow optimization, and real-time monitoring. And we consider multi-tenancy, security, and machine learning for a well-rounded solution.

2) Social media monitoring using ELK Stack , IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES) , 2022. This project builds a social media monitoring tool for small businesses using ELK. It analyzes data in real-time, helping them understand trends and gain valuable insights. It even has potential as a security system! The future looks bright – so we plan to add machine learning and handle larger datasets, making it even more powerful and applicable to a wider range of businesses.

3) Cyber Attacks Detection Using Open Source ELK Stack , 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) , 2021. This ELK-based project delivers a powerful, proactive cyber defense system against APTs (Advanced Persistent Threats). It utilizes automation (e.g., auto-hash querying) and threat anticipation for network and endpoint security. The system boasts APT detection, geolocation analysis, real-time threat searches, and machine learning anomaly detection within Elasticsearch. So for future scope we decide to enhancements include broader threat intelligence, improved machine learning, and larger scale implementation.

4) CloudProcMon: A Non-Intrusive Cloud Monitoring Framework , IEEE Access (Vol. 6) , 2018. This research introduces CloudProcMon, a novel cloud monitoring framework. Unlike traditional methods, CloudProcMon gathers data directly from the host operating system (OS) without additional software, making it lightweight and scalable. This non-intrusive approach minimizes system strain while proving efficient. The study demonstrates the effectiveness of non-intrusive monitoring compared to intrusive methods. They successfully collected data from the OS's Procfs and linked it to a central cloud controller. Future work focuses on expanding the range of metrics collected using CloudProcMon. This will further assess its potential to meet the needs of both cloud users and providers, all while keeping the impact on system resources minimal.

5) The Importance of Monitoring Cloud Computing: An Intensive Review, Proc. of the 2017 IEEE Region 10 Conference (TENCON), Malaysia, November 5-8, 2017. Recent advances in hardware and software of cloud computing are putting tremendous pressure on the administrators who manage these resources to provide uninterrupted services. Monitoring cloud computing plays a significant role in enhancing the quality of cloud computing services. Regular monitoring may help to adaptively scale resource utilization and determine service problems. It also helps to explore the usage patterns of different end users. System administrators should be familiar with cloud services monitoring and network tools. Previous studies considered different components of cloud computing such as properties, technology, privacy and security issues. This study reviews cloud monitoring tools that can help in monitoring and processing of data centers. In particular this study discusses the essential and desirable features of the existing cloud monitoring tools. Both open source and commercial tools were surveyed and their salient features were highlighted.

6) True Real-Time Change Data Capture With Web Service Database Encapsulation , 2010 IEEE 6th World Congress on Services. This research tackles the challenge of achieving real-time data capture with Change Data Capture (CDC) technologies. Traditional CDC methods, like log scanning and timestamps, rely on polling the data source for changes. This inherent polling creates a delay, hindering true real-time functionality. The study proposes a new approach to overcome this limitation. They suggest encapsulating the data source with a layer of web services. These web services would act proactively, pushing any data changes to the target destinations in real-time, eliminating the need for polling. Additionally, we will introduce a framework specifically designed to enable this real-time flow of data.

III.   PROPOSED SYSTEM

This article explains how to use the ELK Stack (Elasticsearch, Logstash, and Kibana) to monitor cloud-based payment gateways in a thorough manner. Utilizing the scalability and security advantages of the ELK Stack, a centralized platform for effective log management, threat detection, and real-time transaction analytics is created. Filebeat, a lightweight shipper, starts the data gathering process by looking for log files holding transaction data at specific locations on payment gateway servers. This guarantees thorough reporting of every transaction made through payment gateways. As the pipeline for data processing, Logstash takes in Filebeat logs and formats them into an organized manner. This include finding pertinent fields, extracting timestamps, parsing raw data, and removing superfluous information. After processing, the logs are sent to Elasticsearch for analysis and archiving.
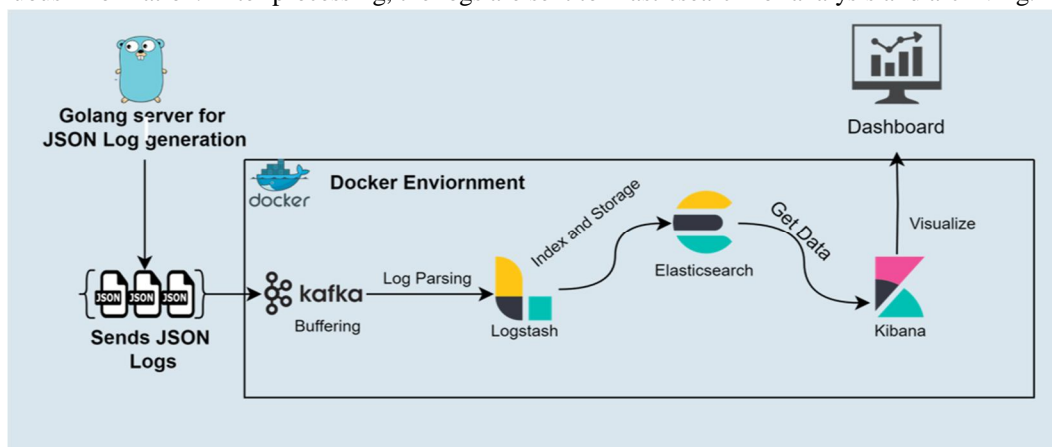

Fig 1: Block Diagram

Elasticsearch is a distributed analytics and search engine that effectively stores massive amounts of data for fast retrieval. To enable quick Kibana querying and analysis, it indexes the processed logs.

The graphical user interface (graphical user interface) for interacting with Elasticsearch data is termed Kibana. Through an intuitive online interface, operators can create bespoke dashboards that show important payment gateway KPIs (Key Performance Indicators) in real-time. Important data including transaction volume, latency, mistake rates, and possible weaknesses in security can be shown on these dashboards. In essence, Kibana gives operators instant access to information about the state and operation of the payment gateway. When handling sensitive financial data, security is crucial. Every step of the data pipeline is equipped with secure communication protocols in the proposed layout to guarantee security

Based of the ELK Stack's renowned horizontal scalability, the system can change to meet changing demands. Elasticsearch and Logstash can easily add more nodes to manage the growing data load as the number of transactions grows.

The approach can be enhanced further through the use of real-time warning methods. Operators can receive alerts about potential issues, such as strange transaction patterns or spikes in error rates, by setting thresholds for crucial metrics in Kibana. This proactive strategy makes preventative troubleshooting easier and reduces the impact of disruptions.

There are several advantages to using the ELK Stack for payment gateway monitoring. Real-time performance insights, centralized log management for improved analysis, quicker payment processing issue troubleshooting, proactive risk identification and mitigation, and the flexibility to scale the monitoring solution to meet transaction volume growth are a few of these benefits. In the end, this comprehensive strategy gives payment gateway operators the ability to guarantee continuous operations, protect sensitive financial information, and provide an exceptional user experience for their clients.

IV. CONCLUSIONS

This well-written SRS document is the foundation for a ground-breaking MaaS platform that will watch out for the financial ecosystem. By utilizing the power of the ELK Stack, the platform goes beyond the constraints of traditional monitoring. Operators obtain a bird's-eye perspective of the payment gateway landscape in addition to real-time transaction analytics. Smooth data flow is guaranteed by the secure and scalable architecture, from lightweight agents' data gathering to Kibana's user-friendly visualization and organized storage. Beyond observation, the suggested method serves as a preventative barrier. Operators will be able to recognize and resolve such threats before they cause interruptions thanks to real-time alerts and the integration of machine learning in the future. This points to a secure online shopping future where seamless user experiences and easy transaction flows are ensured.

V. FUTURE SCOPE

Future objectives for the dashboard include adding some further sources of information that will cover a wider range of financial instruments, such as We aim to enhance the capabilities of our data visualization dashboard by expanding its data sources to include commodities and foreign currency markets. Furthermore, we intend to increase our support for developing tokens and improve the coverage of cryptocurrencies by adding blockchain networks and emerging tokens. We will prioritize performance improvement by focusing on distributed computing and caching to minimize data latency and handle larger datasets more efficiently. With these advancements, we hope to transform the dashboard into a valuable resource for financial experts in a data-abundant environment.

REFERENCES

[1] FEDARGOS-V1: A Monitoring Architecture forFederated Cloud Computing Infrastructures , IEEE Access(Vol. 10) , 2022

[2] Social media monitoring using ELK Stack , IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES) , 2022.

[3] Cyber AttacksDetection Using OpenSource ELKStack , 13th International Conference onElectronics, Computers andArtificial Intelligence (ECAI) , 2021

[4] CloudProcMon:A Non-Intrusive CloudMonitoring Framework , IEEE Access(Vol. 6) , 2018.

[5] The Importance of Monitoring Cloud Computing: An Intensive Review, Proc. of the 2017 IEEE Region 10 Conference (TENCON), Malaysia, November 5-8, 2017

[6] True Real-Time Change Data Capture With Web Service Database Encapsulation , 2010 IEEE 6th World Congress on Services.

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089   (24*7 Support on Whatsapp)