indium
Make Technology Work

Big Data Security using Kerberos for a leading Mobile engagement provider

Digital Services

Success Story

Client

The client is a leading mobile engagement and communication provider with 18 years of experience in connecting 1500+ clients with their customers across industries such as BIFS, DTH, government, automotive, retail and FMCG, and e-commerce.

Overview

Every day, the client enables sending 150-200 million SMSs with growth expected to reach 500 million in the near future. Given that the legacy Oracle and MySQL infrastructure was unable to scale up to meet its growing needs, the client migrated to a Big Data platform capable of exponential growth. Indium Software was commissioned to architect a security solution at par with their other data infrustructure. The client wanted to establish a proper authorization framework which would defend it from external attack and enable it to set specific privileges for internal users to protect data from any unauthorised users.

Status Quo

Every day, the company enables sending 150 million SMS, and on special occasions the number goes up to 200 million. It expects a growth to 500 million every day in the near future.

Their existing solution on Oracle and MySQL was unable to scale up to meet the growing customer needs. Hence, they scaled to a Big Data platform as that gave room for exponential growth. Once the migration was completed, the company felt it needed a security set up similar to the one on RDBMS. Though Hadoop environment was safe from external threats, it wanted to provide proper authorization and privileges to internal users to protect data from any potential threats.

Why Indium Software

The client approached Indium Software for database migration initially. Once the migration was complete, during a feature to feature check between the existing RDBMS-based system and the Big Data technology-based platform, the company was convinced that the system was safe from external threats. However, they felt the need to protect data from internal users as well.

Data security experts believe that while external threats can be prevented with sufficient security measures, internal ones are harder because many times, the breach is unintentional. Information Security Forum (ISF) classifies internal security threats into three categories:

- Malicious

- Negligent

- Accidental

Business
Big Data Security

Domain
Mobile Engagement

Tools
Hadoop, Cloudera, Kerberos, Ranger

Key Highlights

- The introduction of the Kerberized security feature integrated with Sentry enabled the client to set privileges and prevent unauthorized access
- A 100% elimination of the external access threats to the data was achieved
- 90% of internal accesses were found to be unauthorized and subsequently cut off

Employees may not understand security related issues and inadvertently leak data, while some breaches could be intentional. Some of the risks can be mitigated by setting appropriate authorization and privileges, thus restricting access on need basis to improve data safety and integrity.

Convinced about Indium Software's capabilities and understanding of Big Data technology, as already witnessed in the way the migration had been handled, the client commissioned Indium Software with the development of its security too.

Business Challenge

Hadoop has an inbuilt security system that protects it from external threats. For internal security, it only allows string-based query and is not suitable for setting authorizations, authentication and privileges. However, since the client believed the RDBMS-type of security was important to restrict access of its 250 plus employees, Indium Software had to explore tools. There was no precedent available to refer to and so it had to devise its own security solution.

Indium Software's Approach

Indium Software studied the existing system to understand the security features and conducted a research of the tools to find the right fit. It revealed the existence of tools such as Kerberos and Ranger which were tweaked to suit the client requirements and boost internal security. However, the

original workflow at various points were affected because of the introduction of Kerberos authentication and had to be modified.

The reports from the existing platform were being sent to the database team. But since enabling the Kerberos security on top of Hadoop, this too had to be modified to provide the database team with access to the reports. An audit log reporting the attempts to access the system was also provided to analyze potential threats and breaches.

Business Impact

- As a result of the introduction of the Kerberized security feature integrated with sentry, the client was able to set privileges and prevent unauthorized access, improving data security and integrity.
- This lead to a 100% elimination of the external access threats to the data.
- Additionally, 90% of the internal threats have also been curtailed, owing to the user access permissions being implemented. The remaining 10% comes from the internal names used who need to have access to the system.
- This system ensured the near elimination of malicious security threats, and significantly reduced the accidental and negligent threats.

📞

INDIA

Chennai | Bengaluru | Mumbai
Toll-free: 1800-123-1191

USA

Cupertino | Princeton
Toll-free: 1 888 207 5969

UK

London

SINGAPORE

+65 9630 7959

🌐

General Inquiries
info@indiumsoftware.com

Sales Inquiries
sales@indiumsoftware.com