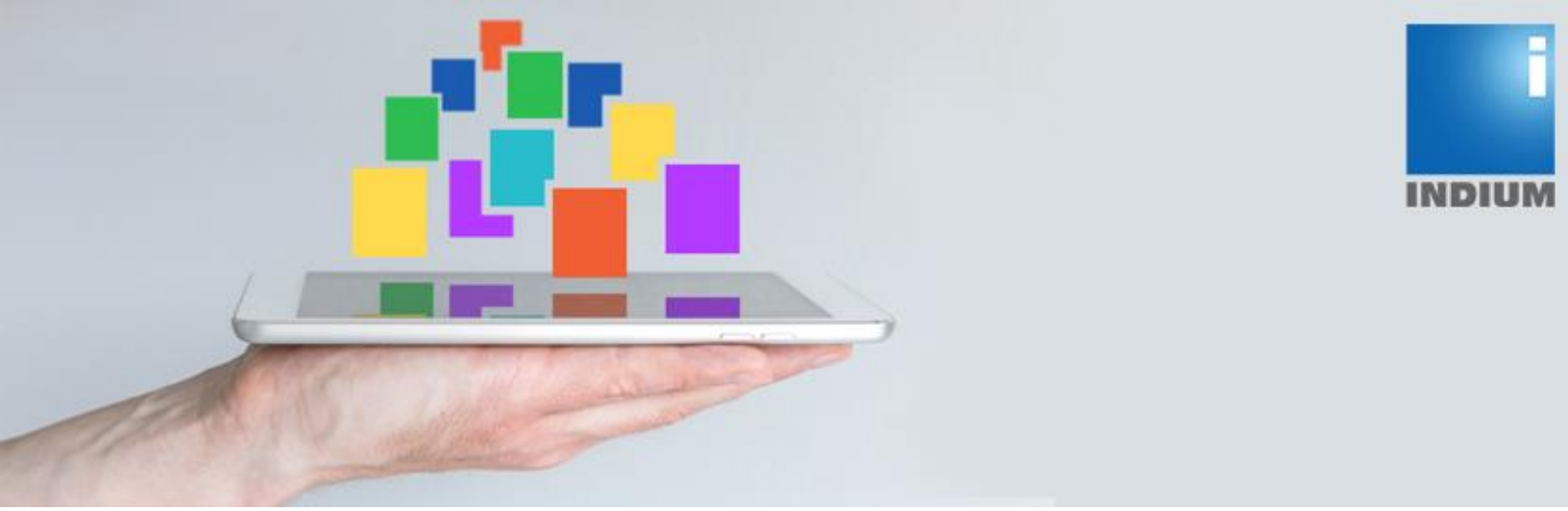

Big Data Security using Kerberos for a leading Mobile Engagement Provider – Success Story

Preventing unauthenticated data access and potential theft from internal users

Application: Using Kerberos to secure 100 million transactions per day.

Services Offered: Permissions and data access restrictions for users similar to RDBMS. Kerberos and Ranger as tools for the security setup. Modification of the original workflow to account for the introduction of Kerberos. Audit log reporting to analyse potential threats.

Tools: Hadoop, Cloudera, Kerberos, Ranger

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. Every day, the company enables sending 150 million SMS, and on special

Key Highlights

Key Success:
Hadoop Security implementation. Elimination of external threats. Near-elimination of internal threats.

Domain:
Mobile Engagement

Duration:
8 Weeks

Team:
2 developers, 1 Architect, 1 Manager

Tools:
Hadoop, Cloudera, Kerberos, Ranger

The Requirement

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

The client approached Indium 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

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's capabilities and understanding of Big Data technology, as already witnessed in the way the migration had been handled, the client commissioned Indium with the

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 had to explore tools. There was no precedent available to refer to and so it had to devise its own security solution.

Indium's Approach

Indium 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.