Chapter 2
Intelligent Broker Design for IoT Using a Multi-Cloud Environment

Balachandar S.
CMR Institute of Technology, Visvesvaraya Technological University, India

Chinnaiyan R.
Presidency University, India

ABSTRACT

Data privacy is the common concern across different enterprises- applications deployed in multi-cloud environment will make it more challenging for the cyber security team to monitor the application traffic simultaneously to prevent any attacks or data leak or data privacy breaches. Handling different data privacy issues always demands for a complete visibility over data flow, which ensures to prevent vulnerability points, and best way to handle sensitive and personal data with right data retention policies and data protection schemes. Articulation of data privacy features from different cloud providers, particularly with their service and deployment model, help to plan cybersecurity teams and build the necessary security analytical models to predict and prevent the data privacy theft and attacks.

INTRODUCTION

The existing outbreak of Covid-19 (Novel Coronavirus) is one of the great examples for data privacy risks (Morgan & Smith, 2020) as per EY (Ernst & Young), it classified into four types and how best we need to handle the data privacy risks. As per Verizon Business 2020 Data Breach Investigations Report (2020 DBIR) published on May 2020, this study shares about 36 confirmed data breaches which were directly related to COVID-19 epidemic. The review also shows 474 data breach incidents from March to June 2020 based on contributor data and publicly disclosed incidents (Miles, 2020). Another major data privacy incident spotted during 2017 in the cloud environment particularly about "WWE" (World Wrestling Environment) database (Massive, 2017) contains information about more than three million

DOI: 10.4018/978-1-6684-6275-1.ch002

user's personal data (e.g., Email, Ages, Gender and) kept in the Amazon S3 Storage (Cloud Storage). The S3 Storage was accessible without user name and password, the database was misconfigured by WWE IT department which created this major incident. Post that WWE utilizes leading cybersecurity firms to proactively protect their customer data. It is utmost important to ensure the data movement across multi cloud servers and databases are safeguarded with right data protection techniques, enable proper data governance in place for the applications () which needs data from different cloud. This document explains different data analysis done for data privacy implementation of sweeping regulations like GDPR (Wikipedia, 2022a) (General Data Protection Regulation) promises well for data security in multi cloud platforms like Amazon Aws, Azure and Google Cloud Platform. We analyze the reviews from different authors and publishers mentioned about data privacy issues in cloud and what sort of regulations should be taken care, also the analysis done for different compliance mechanisms.

In Section III we cover the functional needs of data protection and handling privacy for cloud server and databases. In section IV we explain the basics of multi-cloud platform and section V we examine the what are different data classification method required for different security compliance. In section VI we will mention about different cloud security tools and its purpose. Section VII will mention about problem relevancy with high level approach and step by step component mapping with known issues. We will share the deployment considerations and issues in section VIII. In section IX we will present our significance and in section X we will share our recommendations and conclusion.

BACKGROUND

Multi Cloud environment is the key trend in the upcoming year as per Gartner 2020 Trends (Gartner, 2020). Gartner is estimating that by 2021, 75 percent of midsize and large organizations will have adopted multi-cloud or a hybrid strategy. This will significantly help integrating different applications for enterprise from their on-premise or private cloud to public cloud or multiple public clouds. The resiliency and service level agreement are thrown to different cloud providers who has to support with right balance of high availability, geo replication and fault tolerance and disaster recovery based on the down-time agreement. the data privacy and data hiding are important when data movement happens across cloud servers or database from on-premise application or cloud-based applications. We will be sharing the key literature reviews for different journals and notes which had been done by some of the researchers.

As mentioned by **Jiangshui Hong et.al (Hong et al., 2020)**, It details out the issues with cloud computing particularly about "Four Layer Cloud Computing Architecture" and how resources are managed in each layer. They also discussed about "Issues" with cloud computing and "Data Security & Privacy" is one of the biggest issues and its pressing matter for many researcher and business organizations. They also mentioned top 10 issues of multi-cloud environment. As referred in **Yunchuan Sun et.al (Sun et al., 2014)** explicitly mentioned about memory database encryption technique for privacy and security of sensitive data in untrusted cloud environment.

As mentioned **(Orekhova, 2022)" paper,** the role of blockchain for IOMT devices and not trusting members on the network (e.g., Healthcare providers, Care Takers). they covered on the data security & privacy of IOMT devices in the cloud platform. They described an algorithm of how a block is added to blockchain with an illustration of EMR (Electronic Medical Records)

Wencheng Sun e.al (Martin, 2018) focused on the security and privacy requirements related to the data flow for Internet of things. They mentioned the Lightweight Private algorithms (DES) which is