SwarmPuffProject

TAIP MSSI 2018-2019

1. Introduction

With the everlasting development of technology and society, data privacy has proven to grow into a pressing issue concerning people all around the world.
According to the General Data Protection Regulation [1], collecting, processing and storing user data without explicit consent is a punishable offense. Moreover, any entity that has even the slightest interaction with the user's personal information has to be able to deliver a structured copy of everything they have collected and the possibility to delete it if the user withdraws his or her approval of the previously mentioned actions. If the data ends up in the wrong hands, the enterprise which stored it has to be able to notify the user of the breach of security he or she was subjected to.
In order to comply with the above mentioned regulations and the more other stipulated in the GDPR [1], many companies have sought ways to improve their system architectures, in order to support monitoring the data access, removing ties between user information and finally cleansing all of it on demand.
For instance, after the Cambridge Analytica scandal [2], Facebook has suffered a severe stock drop and faced serious consequences for collecting user data and offering it for processing to other entities, such as commerciants and advertisers without the user's explicit consent. In order to avoid legal repercussions, they are said to have improved their confidentiality policy by presenting the users choices regarding what they want to share and offering them the option to view and delete the data they store [3]. Nonetheless, some speculate that "Facebook still holds the reins when it comes to your personal data" [5], since "Facebook delved into design tricks to keep from losing our data" [4]. The way options were laid out is encouraging the users to speed through the process of deciding what's best for them by highlighting the "I accept the terms and conditions" button, whilst making the decline course of action almost untraceable[4][5].
Even though GDPR is a regulation promoted by the EU, it does not apply only to enterprises that have legal residence in EU, but to all companies that process data belonging to EU citizens. In the light of this, Google, which has its main headquarters in Mountain View, California, is also a subject that must comply to the these laws when providing any of its services, such as Gmail, Google App Engine, Google Analytics, Youtube and many others. Besides the explicit consent agreements, the enterprise has also worked on its ads mechanism, by making tarketing less

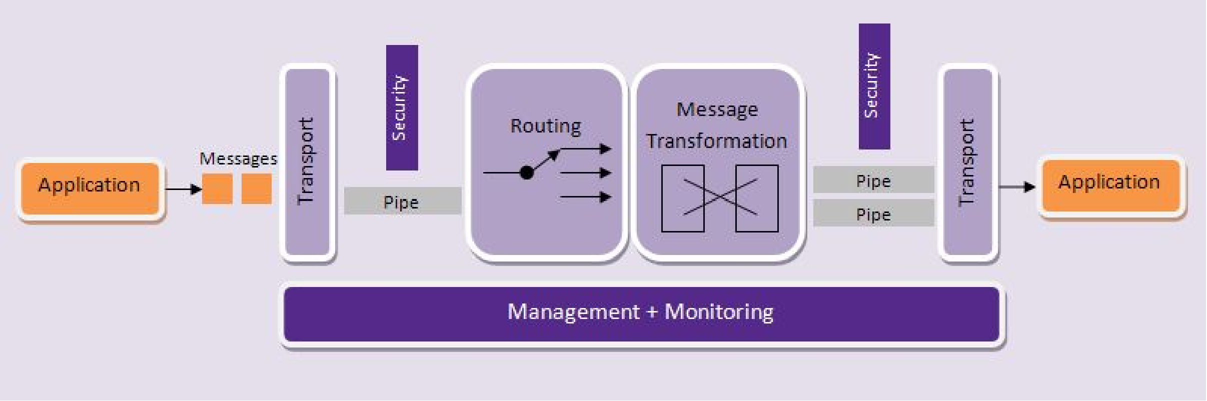
aggressive and imposing more severe measures when it comes to teenagers using their services [6].

No matter the solutions enterprises come up with at this point, if data confidentiality was breached once, their systems are vulnerable for more to come in the future. That is why, according to the “Privacy by Design” principles [7], a digital processing unit must be built in order to anticipate and foresee data breaches and integrate confidentiality in its components from the beginning, not as a last minute extension. This paper promotes an alternative cloud integration technology, Swarm ESB [8] [9], that centers on protecting data confidentiality, while decoupling complex systems in small entities that can coordinate themselves in order to work with as little user data as possible. Moreover, any application designed on the core architecture of Swarm ESB is guaranteed to comply with almost all GDPR requests [18], by making it easy for users to know which data is collected and with what purpose and by offering useful tools for enterprises to develop access monitoring and data removal features.

2. Activity in this field performed by others, methodologies used, evaluation methods, results

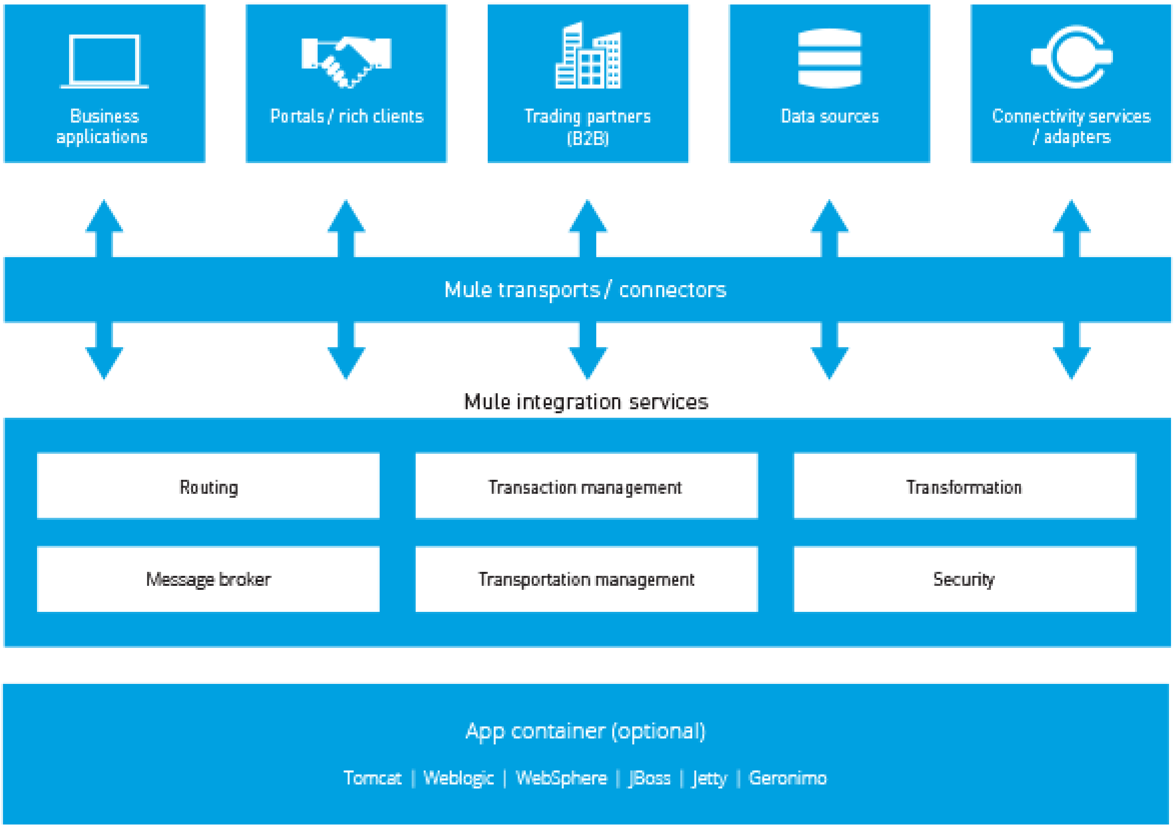
There are various architectures that could be approached in designing complex systems, but only a few consider privacy as a main concern. For instance, there are a few Enterprise Service Bus [11] implementations that offer iPasS (Integration Platform as a Service [12]) solutions, centered on confidentiality. Some of the most remarkable are Mule ESB [13], WSO2 ESB [14], Talend ESB [15] and Swarm ESB.

WSO2 ESB integration solution approaches confidentiality by implementing sixteen security scenarios inspired from the web services security policies. Some examples are the UsernameToken, Non-repudiation, Integrity, Confidentiality and Kerberos Token-based Security scenarios [21]. Each one of them uses either digital certificates or keys in order to verify the identity of the sender and the authenticity of the message.



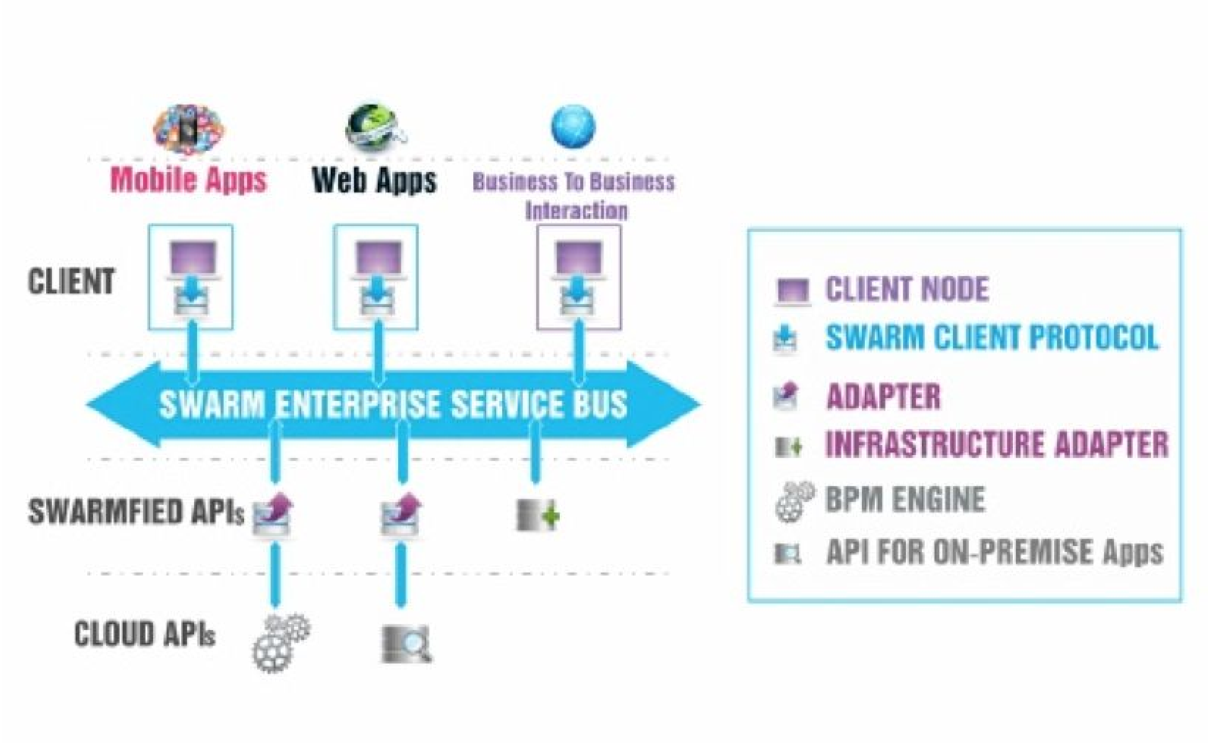
WSO2 ESB Architecture

Mule ESB integration solution offers resource access constrained by several filters and policies, while preventing sensible data exposure by using encryption, digital signatures and access control techniques for APIs usage. Any request is authenticated, authorised and validated by using the credential vault [20], which stores all the encrypted private data required for communicating securely with other entities.


Business applications
Portals / rich clients
Trading partners (B2B)
Data sources
Connectivity services / adapters
Mule transports / connectors
Mule integration services
Routing
Transaction management
Transformation
Message broker
Transportation management
Security
App container (optional)
Tomcat | Weblogic | WebSphere | JBoss | Jetty | Geronimo

Mule ESB Architecture

In order to understand the way Swarm ESB helps us keep data safe from the wrongfully intended, we must first approach the concepts behind it. Swarm communication is a pattern of sending and processing messages between adapters. An adapter is a server side software node that offers a specialised functionality of the system, which can be used only through a swarm. Usually, communication in an ESB implementation takes place between complex entities, that process simple messages. This leads to an overwhelming use of resources. To prevent that from happening, Swarm ESB pictures messages as “smart” entities, capable of taking over some of the workload, by being routed between specialised components. As a concept, a swarm is a gathering of messages altogether, that have a role beyond of just storing information, which helps reduce the complexity of distributed systems, offering scalability, disponibility, decoupling between host systems that have many guest systems and parallel use of resources [16].



Swarm ESB Architecture

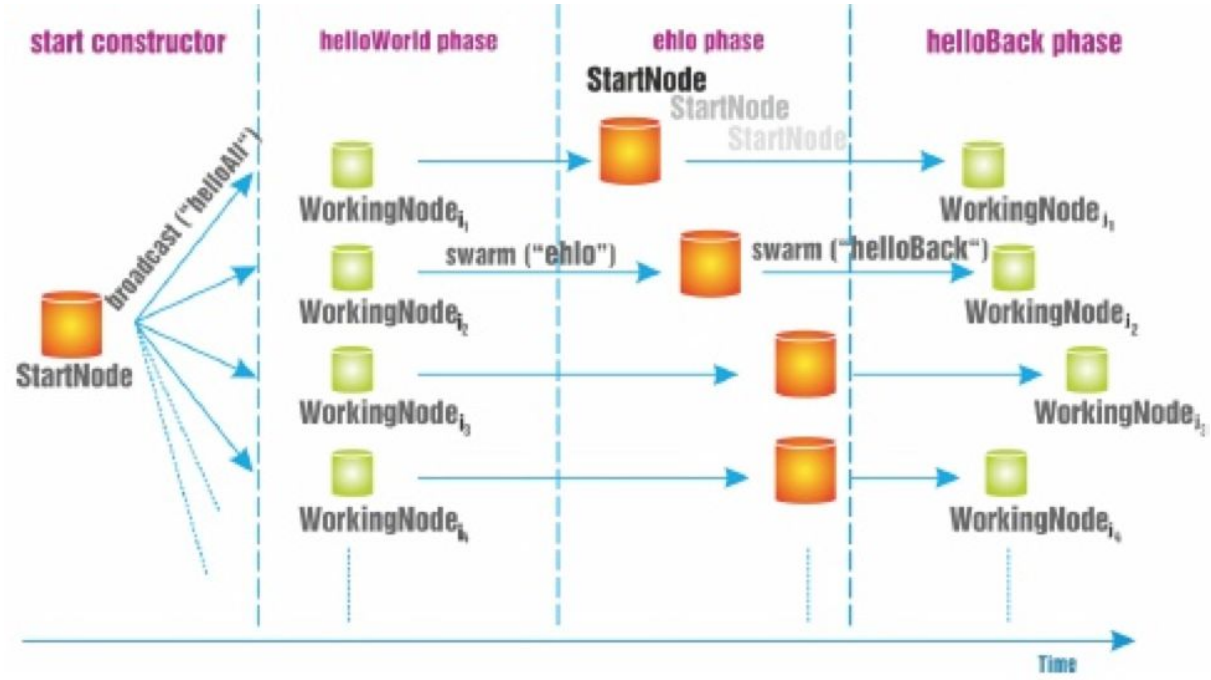
The integration strategy proposed by Swarm ESB is one of the few that cover all privacy principles, by proposing the usage of executable choreographies. The implementation of this concept turns formal contracts between organizations in code executed by every communication participant. Therefore, choreographies are not envisioned anymore as simple descriptions of an agreement between various organisations. They describe the order of interaction and its content in an executable context. The standard classification contains three categories, according to [24].

Verified Choreographies are accompanied most of the time by automated methods of verifying usage of user data. A privacy advantage of using them is the capability of monitoring the data stream directly in the integration layer, which is logically separated by the processing code, found in adapters.

Encrypted Choreographies use various control access mechanisms, with the purpose of identifying and authenticating the key entities that communicate through swarms. Usage of data encryption algorithms for storage by every organization prevents personal data breaches and distribution. Moreover, communication between nodes and swarms supports some encryption and privacy centered protocols, that ensure protection against Man in the Middle attacks.

Serverless Choreographies incapsulate advantages from the other two categories, by adapting them in order to be appropriate for deploying in a public cloud, which offers monitoring and full automation of processes capabilities. Developing a system based on this type of executable choreography results in less people with physical or administrative access to the data stream.

Since executable choreographies are the key principle of the “Privacy-Integration” model Swarm ESB proposes, developers using it are encouraged to use public cloud resources. The level of privacy provided would equal the one guaranteed by instantiating a private server for every user.



Choreography example

Swarm ESB offers various tools in order to encourage the development of applications centered on privacy, like the access control library that allows granting different permissions to users over resources. Another library can be used to remember the permission tree, the entities relationships and the access logs by storing them in a Redis [17] instance. Data breaches can be signaled by configuring one of the bundled libraries.

Another capability Swarm ESB offers is the possibility of building security contexts, by restricting access to resources. Any user can be granted a certain level of trust (following the Biba pattern) and a specific tree of permissions (following the Bell La-Padula pattern), approach that prevents unauthorised access [19].

In order to decide between the potential integration solutions, we compared them pertinently using some decisive metrics.

Criteria	Mule ESB	Talend ESB	WSO2 ESB	Swarm ESB
Easy to use environment	+	+	+	-
Inclusion of necessary dependencies	+	+	+	-
Dedicated components, easy to use	-	+	-	+
B2B components	+	-	-	-
Usage of a well known language for message manipulation	-	+	+	+
Posibility of application debuging	+	+	+	-
Tools for managing and monitoring	+	-	+	-
Documentation/ Tutorials / Articles	+	+	+	+
Charge free support 24/7	+	+	+	-
Dedicated components for message transformation	+	-	+	+
Intuitive configuration of database intraction	-	+	+	-
Extensibility	+	+	+	+
Flexibility	+	+	-	+
Reduced and previsible costs	-	+	+	+
Error hadling mechanisms	+	+	+	+
Compatibilty with a large number of operating systems	+	+	+	+
Tackles solutions for “throttling”	+	-	+	+
Open Source	-	+	+	+
Methods to assure data confidentiality	-	-	-	+
Methods to secure communication	+	+	+	+

Comparison between ESB-based technologies

As we can see, Swarm ESB brings numerous advantages in regards to the analysed criteria. Nonetheless, its most important qualities are its confidentiality mechanisms in regard to data privacy and secure communication. Therefore, we chose this technology to work further with in developing our project.

3. Important names in the field, research teams

The core of Swarm ESB is developed as the main outcome of the open source project, PrivateSky. A list of the team members can be found here: https://profs.info.uaic.ro/~ads/PrivateSkyEn/team-3

4. Related articles and books

1. G. Calancea, L. Alboaie, A. Panu, A SwarmESB Based Architecture for an European Healthcare Insurance System in Compliance with GDPR, 19th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT-18), Jeju, Korea 2018
2. I. Stanescu, L. Alboaie, A. Panu, Blockchain and Smart-contracts Modeled in a SwarmESB Ecosystem, 19th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT-18), Jeju, Korea 2018
3. L. Alboaie. Towards a smart society through personal assistants employing executable choreographies. At 26th International Conference on Information Systems Development, Cyprus, 6-8 September 2017.
4. Sinica Alboaie, Ioana Bogdan, Lenuta Alboaie, and Mircea-Florin Vaida. Operations on encrypted data in an ORM made for encrypted choreographies. At 16th RoEduNet Conference: Networking in Education and Research, IEEE 13th International Conference on Intelligent Computer Communication and Processing, Târgu-Mureş, Romania, September, 2017
5. Sinica Alboaie, Lenuta Alboaie, Mircea-Florin Vaida, and Cristina Olariu. Executable choreographies applied in OPERANDO, (extended paper). In Computer Science Journal of Moldova, 2016. Vol. 24, Issue 3, p417-436., 20p, 2016
6. Sinica Alboaie, Lenuta Alboaie, and Mircea-Florin Vaida. Web service transformations in a federated Enterprise Service Bus based on executable choreographies. At Proceedings of the Conference on Mathematical Foundations of Informatics MFOI2016, July 25-29, Chisinau, Republic of Moldova, 2016
7. Lenuta Alboaie, Sinica Alboaie, and Tudor Barbu. Extending swarm communication to unify choreography and long-lived processes. At 23rd International Conference on Information Systems Development (ISD2014 Croatia), 2014

8. Lenuta Alboaie, Sinica Alboaie, and Panu Andrei. Swarm Communication - a Messaging Pattern proposal for Dynamic Scalability in Cloud. At 15th IEEE International Conference on High Performance Computing and Communications (HPCC 2013). Zhangjiajie, China, November 2013

5. Relevant links. Resources and tools available

[1] EU General Data Protection Regulation. [Online]. Available: https://www.eugdpr.org/
[2] Cambridge Analytica. [Online]. Available: https://cambridgeanalytica.org/
[3] What is General Data Protection regulation? [Online]. Available: https://www.facebook.com/business/gdpr
[4] Josh Constine, A flaw-by-flaw guide to Facebook's new GDPR privacy changes. [Online]. Available: https://techcrunch.com/2018/04/17/facebook-gdpr-changes/
[5] Rachel England, Facebook explains how it will comply with the EU's GDPR. [Online]. Available: https://www.engadget.com/2018/04/18/facebook-explains-eu-gdpr-compliance-privacy-data/
[6] Allison Schiff, This Is How Google Is Preparing For GDPR. [Online]. Available: https://adexchanger.com/privacy/this-is-how-google-is-preparing-for-gdpr/
[7] Ann Cavoukian, Privacy by Design The 7 Foundational Principles (2011)
[8] Sinica Alboaie, What is Swarm ESB? [Online]. Available: https://github.com/salboaie/SwarmESB
[9] Private Sky Developer Guide (v0.5), 2017
[10] Cristina-Georgiana Calancea, Modelarea sistemului de asigurări de sănătate conform prevederilor GDPR, 2018
[11]Kumar Phani, MOM vs ESB. [Online]. Available: http://javaresolutions.blogspot.ro/2014/08/mom-vs-esb.html
[12] Margaret Rouse, iPaaS (integration platform as a service). [Online]. Available: http://searchcloudapplications.techtarget.com/definition/iPaaS-Integration-platform-as -a-service
[13] MuleSoft Inc.(2017), What is Mule ESB? [Online]. Available: https://www.mulesoft.com/resources/esb/what-mule-esb
[14] WSO2 Inc.(2017), WSO2 Enterprise Service Bus. [Online]. Available: http://wso2.com/products/enterprise-service-bus/#Features
[15] Talend ESB. Talend. [Online]. Available: http://www.talend.com/products/esb
[16] Lenuta Alboaie, Sinica Alboaie, and Panu Andrei. Swarm Communication - a Messaging Pattern proposal for Dynamic Scalability in Cloud. At 15th IEEE International Conference on High Performance Computing and Communications (HPCC 2013). Zhangjiajie, China, November 2013, http://www.academia.edu/15349768/Swarm_Communication_-_A_Messaging_Patter

n_Proposal_for_Dynamic_Scalability_in_Cloud
[17] Redis. [Online]. Available: https://redis.io/
[18]L. Alboaie. Towards a smart society through personal assistants employing executable choreographies. At 26th International Conference on Information Systems Development, Cyprus, 6-8 September 2017.
[19] Sinica Alboaie, acl-magic: magically simple but powerful ACL (Access Control List) node.js module. [Online]. Available: https://www.npmjs.com/package/acl-magic
[20] Mule Credentials Vault. [Online]. Available: https://docs.mulesoft.com/mule-user-guide/v/3.6/mule-credentials-vault
[21] WSO2 Inc. (2017), Security Implementation. [Online]. Available: https://docs.wso2.com/display/DSS322/Security+Implementation