Abstract

The internet is attracting more and more users every day. The majority of these users are mobile users. Which results in an overload of demand to smartphone apps. That is the reason why the app stores count more than two million apps. Users tend to use apps which function as an all-in-one solution, the so called super apps. Super apps are a set of services provided by member apps. These new generation of apps come in handy but also gather a lot of information of their users. On one side there is the primary data which is the sensitive data provided by the user, on the other side gathers the app quantitative data. The amount of data provided by super apps brings privacy and security concerns. These apps gather data about user habits such as lifestyle and purchasing behavior. Super apps are often targeted for malicious attacks that have the objective to reveal individual private data from millions of users.

So the question that needs to be answered is, How can user data be secured? To do so, there is need for a framework that enables developing a super app using privacy by design principles. This can be done by using different technologies which help to securely store data.

The challenges that go with these technologies are divided in two categories, namely scalability and disaster recovery. The difficulty with scalability is horizontal scaling. When adding new processors they will require a process of provisioning the new SGX keys. A second challenge is that data can go lost when a processor fails. Which brings up the question, how can lost data groups be recovered?

When the framework is put into practice, super apps would be more feasible for privacy regulations such as European GDPR. The framework prevents privacy loss. So the success of this architecture could make new business models possible.