FACTORS CONTRIBUTING TO THE SUCCESS:

Super app in south Asian countries become so demand could their popularity extend in US and European countries.

These applications consolidate services, miraculously removing the user from the plethora of different apps that clog up their mobile devices and desktops. Furthermore, why keep a big number of passwords for each application separately and then search the application library for the one you need right now when you can use a single application that combines all of this information? This is the primary question that huge corporations are pondering in order to expand their market share. There are numerous reasons why behemoths like Amazon, Facebook, and Google are attempting to build universal portals that connect disparate services. It is beneficial to both the user and the company. It is the capacity for users to solve multiple problems using a single application. In practise, this implies fewer issues with registration and login.

This represents a significant reduction in the costs of developing and maintaining the application in the future for business owners. Launching a Super Application needs fewer resources from the development team and reduces the number of potential issues that can arise during the development of several applications. The "all-in-one" method is, perhaps, the most compelling rationale for the success of these applications. Creating a one-size-fits-all place for everything a modern user requires is almost certain to be a success. Your success is only a matter of time if you have the correct strategy, business plan, and development team in place. The result is more audience reach, who are more likely to make in-app purchases with less effort.

**Four key reasons for super app success:**

* Mobile experience
* Homogeneous market
* Unbanked population
* Government support

Mobile experience:

The most influencing factor is that not so long ago, mobile devices had a limited storage issue, preventing users from downloading multiple apps and shaping their behavior towards the installation of those that offer a variety of services and offerings in one place.

Homogeneous market:

Most of the Asian countries have a lot in common in terms of culture. This impacts the homogeneity of markets, allowing different businesses to operate in several countries in the region and offer uniformed services. So, when supper apps were introduced, the demand for services they offered quickly spread to the whole region, contributing to the rise of super apps popularity.

Unbanked population:

It is 73% of the Southeast Asia population is not exposed to the banking system. Now they are mostly depending on online transaction. Their day today activities are becoming easier of super app.

Government support:

Because government looking to connect every citizen, super app fulfilled that need. By that they gained government support. They have all the chances to replace traditional ID documentation.

CHALLENGES FOR SUPER APPS:

From a cyber-security perspective, protecting Super Apps and the people that use super apps isn’t easy. On the one hand, the makers of super apps believe that the key to driving higher engagement, customer loyalty and ARPU growth comes from presenting the user with related services inside a single app experience. Can’t argue with that. On the other hand, to achieve that, super apps have to integrate and allow an unprecedented level of third-party components – like BNPL, Deals, Loyalty, or P2P market-buying functions – inside the app to operate in whatever way that component is designed to operate. Uber says it all below with their recent announcement about relying on many other 3rd party providers for major parts of the super app. As a cyber-security professional, this makes you cringe. This means that the exploitable attack surface inside a super app is much larger than a single-purpose app. In a single-purpose app, the developer (and the security professional) has full control over the workflows, APIs, network calls, read/write functions, etc. In a super app, more of these basic functions are left to 3rd parties and components that weren’t necessarily designed to work together. And that usually translates to a greater risk of leaking sensitive data, excessive exposure of APIs, security misconfiguration, all of which can cause real headaches in protecting users and revenues.

* The Leaky Bucket Problem of Super Apps:

Assume you have a single app that does everything. Awesome. However, in order for the app to function, the user must enter a large amount of data and the programmer must connect to a variety of external services, which is significantly more than a standalone app. A super app's functionality and data collection and use can often go far beyond that of a standalone app, and the super app's developer may not have complete control over how the "other" elements in the app, such as mobile payment, peer-to-peer lending, money transfers, mobile wallet, deals, redemption, and other functions, store, share, protect, or transmit personally identifiable information (PII), transaction data, payment, and health-related information, user behavior, and other functions store, share, protect, or transmit.

* Using One Consistent Security Model Inside a Heterogeneous Super App:

Consider a super app as a big pot of seafood gumbo, with each component launching, connecting, writing, reading, initiating, originating, or terminating using a diverse "pot" of technologies, standards, protocols, methods, data formats, and storage types delivered in a single app to the mobile end-user. Developers and security professionals may not have the time, competence, or controls to accept only those components that are suitable with their chosen security model in the arms race to integrate more new offerings and mobile services into the super app.

* Super app gives both user and hacker more to do:

A super app producer has no control on the security posture of the user's device, and no guarantee that the software will be launched by a genuine user or on a real device, as with all consumer mobile apps. Super app creators often don't account for the bad or malicious user, hacker, or even friendly security researcher while designing their apps for real users. We've seen code scanning companies have a field day with Super Apps, running them on jailbroken or rooted devices, devices infected with mobile malware, or older operating systems that don't have the latest OS security upgrades.