

***Research Report***

“Server Industrial Problem in Cambodia”

Lecturer : Mr. Dinesh Kumar

Prepared by : Kheng Pitou

Date : Aug 29, 2021

**Abstract**

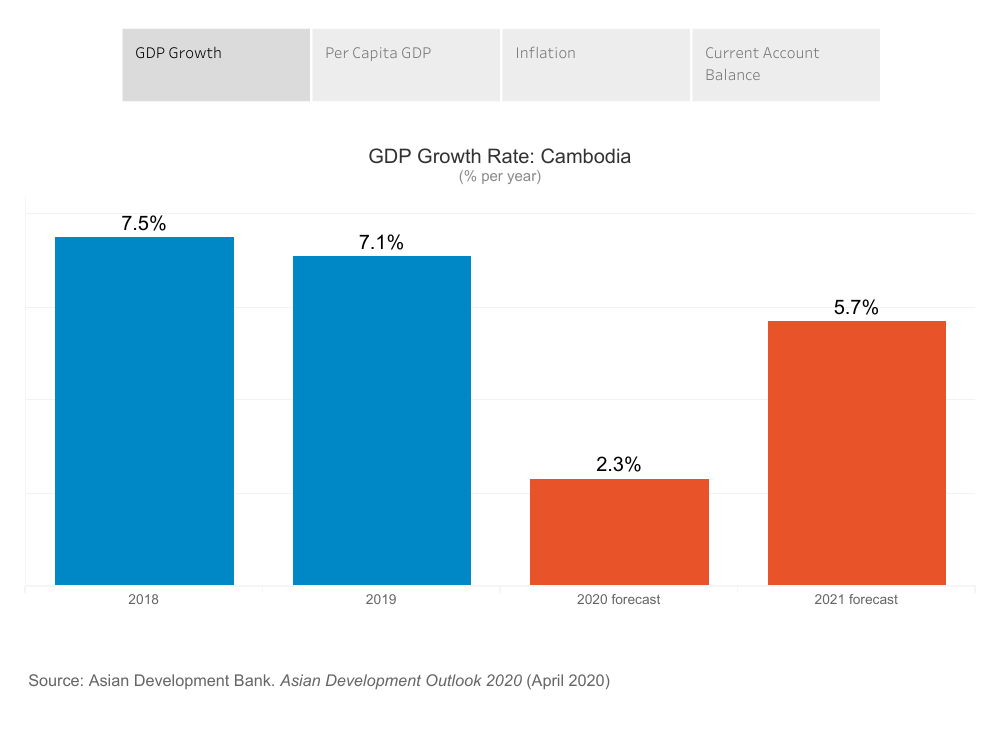
Cambodia is a developing country, which has a rapidly growing economy in each industry. In the past, most entrepreneurs were less knowledgeable about keeping data secure, compared to now; however, the younger generation of entrepreneurs still sometimes have lost their critical data to the hackers as well as their competitors’ company. As a correspondence, the data insecurity has become popular and controversial among business, bank, and many industry sectors in Cambodia.

In this report paper, we are going to study in detail the root causes of data insecurity, the majority of enterprises’ concerns, and proposed solutions, connected with modern technology, simultaneously.

**Table of Contents**

1. Introduction
2. The majority concerns of enterprises in keeping data
   1. Sensitive data in financial records
   2. Lacks of experts in Cloud specialists
   3. Expensive of third party cloud providers
3. Proposed Solution
4. Conclusion
5. Reference
6. **Introduction**

According to [OpenDevelopment Cambodia](https://opendevelopmentcambodia.net/topics/sdg-9-industry-innovation-and-infrastructure/), they have shown the Cambodia development’s graphics from the 2018 till 2021 forecast. The key driver to future growth is either the role of industry or small and medium enterprises (SMEs). Besides, the World Bank found in a May 2019 report that Cambodia’s economy performed better than expected in 2018. Growth for 2018 was 7.5%, a four-year high, compared to 7% in 2017. This economic growth, the highest in the region, is primarily due to the rapid expansion of exports and a surge in Foreign Direct Investment.



Due to the World Bank’s figure above, we can do self-reflection of the size of data growth in each industry. Most importantly, the field such as banking industry, they have a lot of critical financial data in the country, which cannot spread to both internal and external Cambodia since it may bring bad effects to Cambodia’s economic growth. The reasons were, firstly the internal competitors, for example, the domestic private finances can defeat national bank and secondly the external countries were able to know the Cambodia’s economic situation and its flow, which is not a good state for the policy issues.

On the other hand, government departments in Cambodia are increasingly embracing data-driven digitisation initiatives in order to become more efficient, accurate and accessible to citizens. For example, the National Bank of Cambodia recently adopted blockchain technology to reduce its interbank transaction costs. The Ministry of Public Work and Transport introduced mobile payments and a QR code-enabled vehicle information database to enhance its users’ experience. Also the Ministry of Health is overhauling its Data Management and National Hospital Systems to make its services more easily accessible. As the benefits of data grow, so do its risks, including data breaches. Balancing them requires proper governance and democratization of data, good data software and data skills. This article explores the current state of Cambodia’s e-governance landscape and enterprises with a particular focus on data-driven technologies, how they are implemented and how public awareness around data is growing thanks to local communities and organizations, as well as recommendations for better data strategies.

1. **The majority concerns of enterprises in keeping data**

Based on statistics, we lack experts in Cloud engineering in Cambodia and require enterprises to hire the specialists to control and guide them to store the data. As a result, big enterprises and SMEs decided to store their data on third party cloud providers such as Google Cloud Provider, Amazon Web Service, Digital Ocean, and etc, instead of keeping their data on hand. By using the third party cloud providers overseas, it’s good because they have the experts to maintain and monitor the issues over our database service, which is no need for us to carry anymore. When enterprises choose to store their data on third parties that means they have to put data overseas because there are no data centers in Cambodia yet. Furthermore, as we’ve known, we have only one data gateway from Cambodia to their data center across the country, which is the root cause that makes it easy for hackers to take those data away and sell to the needed person. Above reason is just a part of all, losing data or insecurity of data also came from the unbelievable infrastructure in the cloud environment. Even though enterprises no need to worry about the Service Level Agreement (SLA) and monitor the issues of cloud providers’ services in terms of technical issues, they still have to construct the infrastructure by themselves, which means they must have at least one experts in this field to do for them, a person who can control the infrastructure and keep contact with the cloud providers. This reason is hard for some of the big enterprises to seek the expertises in Cambodia at an appropriate price. What’s more, as recently rumors, the Cambodian government wants to release the data gateway’s law to restrict the data traffic though it’s still not public, that was the thing for enterprises to consider beforehand.

**2.1. Sensitive data in financial records**

Cambodian law contains no laws or regulations that specifically address privacy rights or the protection of personal information collected from individuals in Cambodia. Although the term “Data Privacy” is yet to be defined by any regulation or law in Cambodia, this term is used in various regulations and general principles relating to data privacy exist in several Cambodian laws. The term “Data Privacy” may include reference to facts, pictures, and/or information or circumstances directly or indirectly related to a specific person.

The digital revolution has exponentially increased the amount of personal information that is collected, processed, and stored. How this data is treated, and the scope of personal privacy, is a fiercely contested issue. While the Cambodian tech sector is still relatively small, data collection and personal privacy remain an important issue for individuals and businesses in Cambodia.

Article 40 of the Constitution of the Kingdom of Cambodia provides:

The rights to privacy of residence, and to the secrecy of correspondence by mail, telegram, fax, telex and telephone shall be guaranteed.

What this “right of privacy” means in practice is left to further laws and regulations, as well as to how courts will interpret that right. There are also references to a privacy right found in a number of sector specific laws. For instance, the Press Law restricts the publication of the identities of minors involved in civil or criminal suits, parties to family law cases, and female (though strangely not male) victims of molestation or rape. There are a number of other privacy provisions related to medical patients and financial institutions, though each are fairly narrow.

Anyways, in Kirirom Institute of technology, there is one virtual company who studies data privacy, which is Coin virtual company. They contacted many enterprises and SMEs in Cambodia to raise all their concerns about their data storing and the solution they wanted. As a result, after appointments with enterprises such as BookMeBus, Morokot, and etc, they have shown that they’re also worried about keeping data on third parties as well because their sensitive data, for example financial records, cannot be shown to their competitors. If the hacker can hack that data, it might lead to a bad situation in their company. Moreover, storing data on the cloud, they have no guarantee for them from hackers, unless their IT department can control the data storage and prepare the environment well.

**2.2. Lacks of experts in Cloud specialists**

Looking more closely, one finds that there are specific challenges at the data and information management level. "Information is not distributed freely among the units. Information is rarely disseminated actively, especially within the 'Behind' ministries. This leads to a lack of resources for data collection, and creates barriers to construct centralized information systems" (NiDA and JICA 2009).

In other words, data and information sources remain fragmented and not properly governed with data policies. The responsibilities across the data lifecycle, from collection, access, usage and sharing remain unclear. This is associated with increased costs in working with data. Data and information need to be properly managed, governed and democratised in order to speed up digital transformation and safeguard sensitive data.

According to the reason above, we really need a person who is knowledgeable to control those sensitive data and know the cloud environment clearly. However, in the cloud engineering sector, there is no advance yet and we still need to hire a third party organization overseas to contact and prepare everythings on cloud environments with the cloud providers company.

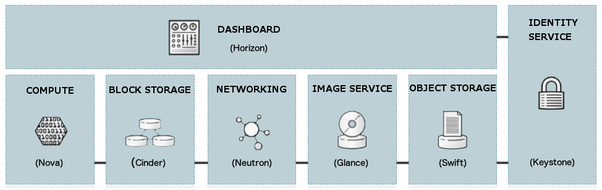
**2.3. Expensive of third party cloud providers**

Storing the data on Cloud such as Amazon Web Service, the enterprises have to pay monthly or yearly subscription on their services. They charges based on the instances (data storage) the users used, the time usage and others services such as back up plan and snapshots, which is the reason for enterprises to spend a high amount of money to comfort those needed services and also need to hire the expertises in high salary to monitor over those services regularly in order to avoid failure of data, high latency or Ddos attack.



1. **Proposed Solution**

Even though most enterprises already use third party cloud providers and don’t want to change though they’re worried about data security because of money when making change, I still believe that my proposed solution will help them a lot to redesign their existing infrastructure security.

Firstly, suppose that the enterprises didn’t use any cloud services yet. We would love to introduce **OpenStack Cloud Platform**, which is a free and open source software platform for cloud computing that is mostly deployed as infrastructure as a service and whereby virtual servers as well as other resources are made available to customers. Even though OpenStack is an open source, we already customize the features on it and make it secure. Here is the OpenStack dashboard:

We will build the infrastructure for the enterprises with high security and more scalability by using the features in OpenStack. For instance, we will prepare the WAF (web application Firewall) to prevent the attack of the hacker and load balancer with multiple availability zones to prevent data failover. We also prepared the network topology for enterprises, which is easy to control in OpenStack Platform. Most importantly, every single service we used, we tried to do the cost optimization for the clients with the standard quality of cloud for them.

Secondly, what if the enterprises already have their own infrastructure? What should they do if they don’t want to spend more to make change? Stop worrying about it. We also have a service to optimize the existing infrastructure with less effect to old infrastructure but obtain high performance, security, and scalability for them. We will study the existing infrastructure beforehand, and then make changes to the inferior services and design the well-prepared infrastructure with cost considerations as well. Our outweighs the third party cloud providers is that we provide the enterprises to keep their sensitive data on hand, no need to purchase license software, expertises issues and more paid on cloud services.

However, if the enterprises or SMEs still want to use third party cloud providers such as Amazon Web Services, what should they do? We also provide services to prepare the cloud infrastructure in AWS services for them as well as to gain the security, high availability, scalability and well prepared environment of keeping data, which is easy for their IT department, especially junior engineers, to continue to control on it. But the enterprises still have to pay for the monthly subscription and pay for monitoring services by themself. They also can hire our services again to monitor their infrastructure, if they want.

1. **Conclusion**

In conclusion, keeping data privacy is vitally important to either enterprises or the government to consider more on it and choose the correct platform to store their data securely. Moreover, they also need to think about the financial cost of regular usage in cloud services as well as the cloud engineers’ salary. Financial records and other records in each department for both enterprises or government are really critical for the economic growth in the country or their own organization. If that data has been lost to the outsider, they might have many stories to solve and might reach bankruptcy for the organization, and policy issues for the government.

1. **References**

* <https://opendevelopmentcambodia.net/topics/sdg-9-industry-innovation-and-infrastructure/>
* <https://www.kas.de/en/web/kambodscha/single-title/-/content/how-data-driven-technology-can-upgrade-cambodia-s-e-government>
* <https://cambodiacounsel.com/data-privacy/>
* <https://www.facebook.com/coin.vc.779>
* <https://www.youtube.com/watch?v=Jg0G1FKPAZU>