

ASSIGNMENT 2 BRIEF

Qualification	BTEC Level 5 HND Diploma in Computing		
Unit number	Unit 16: Cloud computing		
Assignment title	Cloud Computing Solutions		
Academic Year			
Unit Tutor			
Issue date		Submission date	
IV name and date			

Submission Format:

Format: A presentation in Power Point format (about 25 pages) and a security manual (in PDF format). You must use font *Calibri size 12*, set number of the pages and use multiple line spacing at 1.3.

Margins must be: left: 1.25 cm; right: 1 cm; top: 1 cm and bottom: 1 cm. The reference follows Harvard referencing system.

Submission: Students are compulsory to submit the assignment in due date and in a way requested by the Tutors. The form of submission will be a **soft copy** posted on <http://cms.greenwich.edu.vn/>

Note: The Assignment *must* be your own work, and not copied by or from another student or from books etc. If you use ideas, quotes or data (such as diagrams) from books, journals or other sources, you must reference your sources, using the Harvard style. Make sure that you know how to reference properly, and that understand the guidelines on plagiarism. *If you do not, you definitely get failed.*

Unit Learning Outcomes:

LO3 Develop Cloud Computing solutions using service provider's frameworks and open source tools.

LO4 Analyse the technical challenges for cloud applications and assess their risks

Assignment Brief and Guidance:

Task 1: Base on the scenario and architecture design in the first assignment provide the implementation. Because of the time constraint of the assignment, the implementation just provides some demo functions of the scenario. The implementation includes two parts:

- A presentation (about 25 pages)
 - which shows which functions are implemented
 - How to config, deploy and test the services (Web application, Database Server, Source code management, server logs..) using service provider's frameworks and open source tools.
 - Images for the built functions
- The source code for the built application

Task 2: The table of contents in your security manual (which should be 500–700 words) should be as follows:

1. Analysis of the most common problems of a cloud computing platform.
2. Possible solutions to these problems.
3. Analysis of the most common security issues in the cloud environment.
4. Discussion on how to overcome these issues.

Summary

Learning Outcomes and Assessment Criteria		
Pass	Merit	Distinction
L03 Develop Cloud Computing solutions using service provider's frameworks and open source tools		
<p>P5 Configure a Cloud Computing platform with a cloud service provider's framework.</p> <p>P6 Implement a cloud platform using open source tools.</p>	<p>M3 Discuss the issues and constraints one can face during the development process.</p>	<p>D2 Critically discuss how one can overcome these issues and constraints.</p>
L04 Analyse the technical challenges for cloud applications and assess their risks		
<p>P7 Analyse the most common problems which arise in a Cloud Computing platform and discuss appropriate solutions to these problems.</p> <p>P8 Assess the most common security issues in cloud environments.</p>	<p>M4 Discuss how to overcome these security issues when building a secure cloud platform.</p>	<p>D3 Critically discuss how an organisation should protect their data when they migrate to a cloud solution.</p>

Table of Contents

ASSIGNMENT 2 BRIEF	1
ASSIGNMENT 2 ANSWERS	7
1. Functions are implemented	7
2. How to config, deploy, and test the services (Web application, Database Server, Source code management, server logs, etc) using the service provider's frameworks and open source tools	7
3. Images and source code for the built functions	11
4. Analysis and give possible solutions for the most common problems of a cloud computing platform.....	17
4.1. Analyze the most common problems which arise in a Cloud Computing platform and discuss appropriate solutions to these problems	17
4.2. Discuss the issues and constraints one can face during the development process	23
4.3. Critically discuss how one can overcome these issues and constraints.....	25
5. Analysis and discussion on how to overcome of the most common security issues in the cloud environment	28
1.1. Assess the most common security issues in cloud environments	28
1.2. Discuss how to overcome these security issues when building a secure cloud platform	32
1.3. Critically discuss how an organization should protect their data when they migrate to a cloud solution.....	34
6. Summary	35
References.....	36

Table of Figures

Figure 1: Configure GitHub – Step 1	8
Figure 2: Configure GitHub – Step 2	8
Figure 3: Configure Heroku - Step 1.....	9
Figure 4: Configure Heroku - Step 2.....	9
Figure 5: Configure Heroku - Step 3.....	9
Figure 6: Configure Heroku - Step 4.....	10
Figure 7: Configure Heroku - Step 5.....	10
Figure 8: Connect Heroku with GitHub success.....	10
Figure 9: Configure Heroku - Step 6 - MongoDB Atlas	10
Figure 10: Configure Heroku - Step 7.....	11
Figure 11: Configure Heroku - Step 8 – Deploy success - View your web	11
Figure 12: Homepage.....	11
Figure 13: Homepage.....	12
Figure 14: Homepage - Escrow Service Verify	12
Figure 15: Product page.....	13
Figure 16: Order page when not yet add the product into the cart.....	13
Figure 17: Order page when has added the product into the cart.....	14
Figure 18: Payment page	14
Figure 19: Feedback page	15
Figure 20: Login/Register page – Login form.....	15
Figure 21: Login/Register page - Register form	16
Figure 22: About ATN page	16
Figure 23: About ATN page	17

Table of Tables

No table of figures entries found.

ASSIGNMENT 2 ANSWERS

1. Functions are implemented

My application is a website that helps ATN company sales management. It has a homepage and six-page others undertake functions differently on this website.

The homepage is the brand face of the company on the internet, which helps visitors quickly find the information or services needed on the site quickly. In addition, it is a place where the website owners can provide necessary information about products, services, etc... to visitors effectively.

On the other hand, the login/register page has a mission to create an account user if that customer not yet an account, and if that customer had an account then also can log in at here. Next, the product page will manage all products of ATN company and can get a database about products on this page to use for other pages. Here, we used a database on the product page for the homepage to create "Top Product". Next, the order page will create and manage orders follow real-time. In addition, the payment will be implemented and manage on the payment page. We also have created a page for the customer can submit feedback about anythings for the ATN company. Finally is the information page about the ATN company - aboutATN. This page contains all information about the ATN company and a video introduction of artists represent the company.

Besides, we also used Escrow Service Verify for purchase safety, you can use our partner LG U+'s electronic payment protection service (Escrow) when you shop with any method including cash. Finally, we also used background music played auto and loop for the homepage. Because time is limited so we can't install this function for all pages. However, we will make improvements in the future for users who have better experiences.

2. How to config, deploy, and test the services (Web application, Database Server, Source code management, server logs, etc) using the service provider's frameworks and open source tools

We use MongoDB to manage database (detail is MongoDB Atlas), Visual Studio Code to implement and try run locally for web application before when give it on the cloud, GitHub to contain and manage all source code for the web application, Heroku to run web application online on the internet.

Configure GitHub

After you log in to Github's success then you will begin creating a new repository (or you can use repository old if before you created it for the project you need). Below is how to implement:

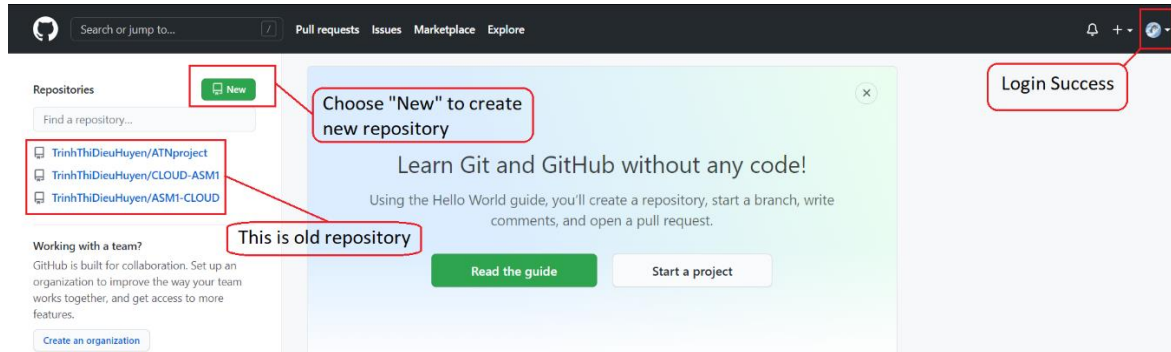


Figure 1: Configure GitHub – Step 1

Create a new repository

A repository contains all project files, including the revision history. Already have a project repository elsewhere? [Import a repository.](#)

Owner * /

Repository name *

Great repository names are short and memorable. Need inspiration? How about [super-doodle?](#)

Description (optional)

☒ **Public**
Anyone on the internet can see this repository. You choose who can commit.

☐ **Private**
You choose who can see and commit to this repository.

Initialize this repository with:
Skip this step if you're importing an existing repository.

☐ **Add a README file**
This is where you can write a long description for your project. [Learn more.](#)

☐ **Add .gitignore**
Choose which files not to track from a list of templates. [Learn more.](#)

☐ **Choose a license**
A license tells others what they can and can't do with your code. [Learn more.](#)

Figure 2: Configure GitHub – Step 2

Next, we will choose the repository just created and then add/upload all source code about our web application into this repository.

Now we configured success for GitHub. Next, we will config for Heroku. In other words, is connect Heroku with GitHub. Below is how to implement:

Configure Heroku

First, we must log in to the Heroku account success, then continue to create a new app for use. Besides, if you are already had an app created before and that app fit with your project then you don't need must create add a new app anymore, you can use directly this app for your project.

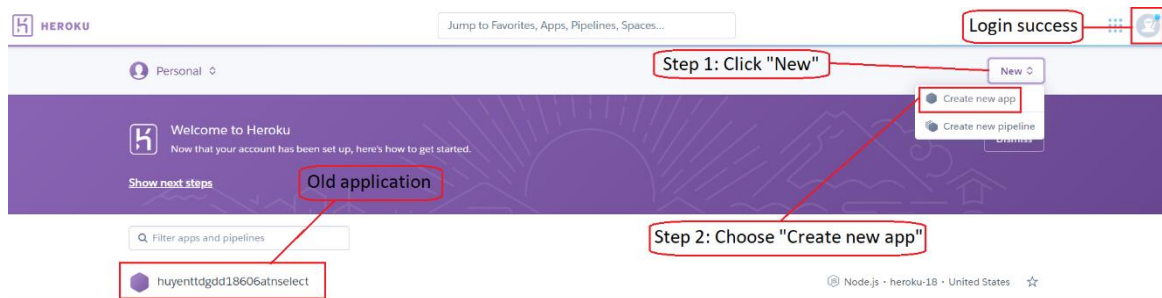


Figure 3: Configure Heroku - Step 1

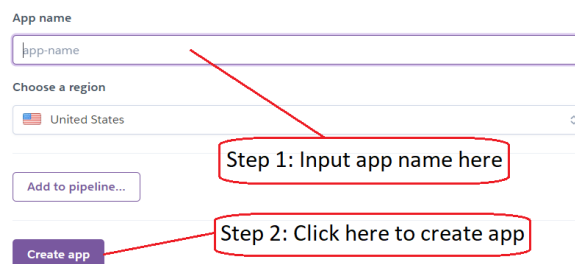


Figure 4: Configure Heroku - Step 2

After the app created, we will continue to connect it with GitHub to get source code to run the web app.

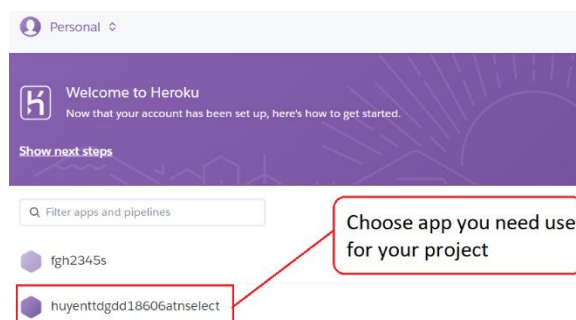


Figure 5: Configure Heroku - Step 3

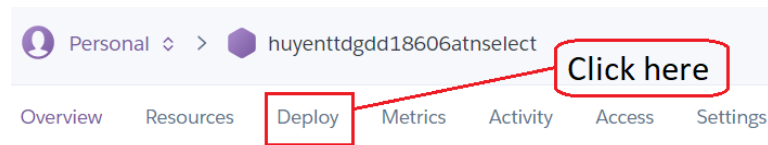


Figure 6: Configure Heroku - Step 4

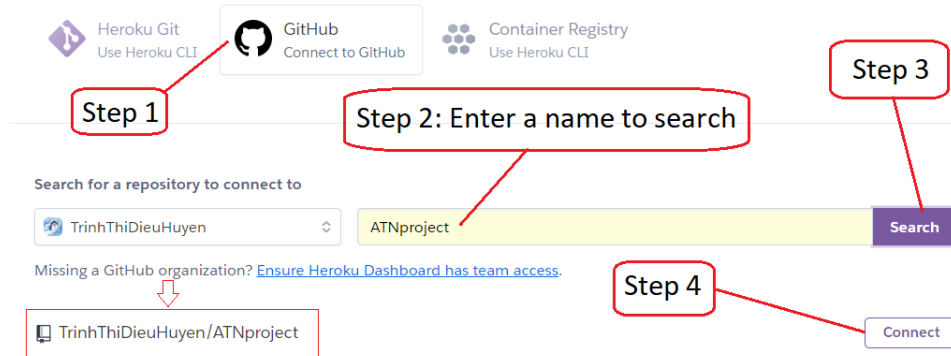


Figure 7: Configure Heroku - Step 5

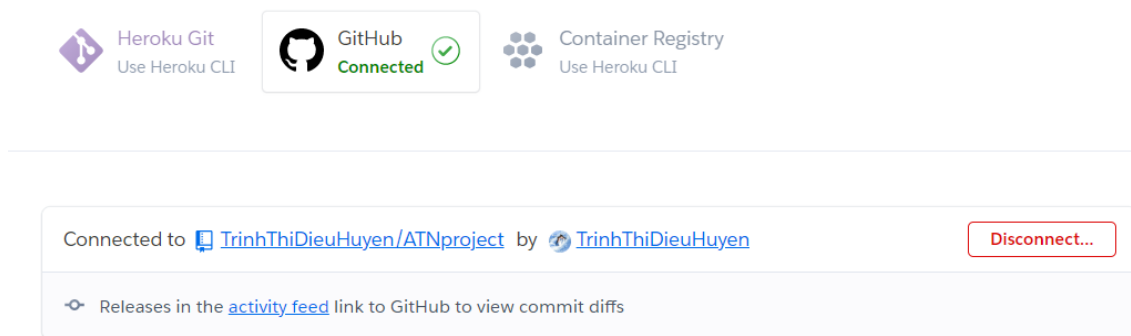


Figure 8: Connect Heroku with GitHub success

Next, we must login and connect success mongoDB atlas with Heroku as below figure (figure 9).

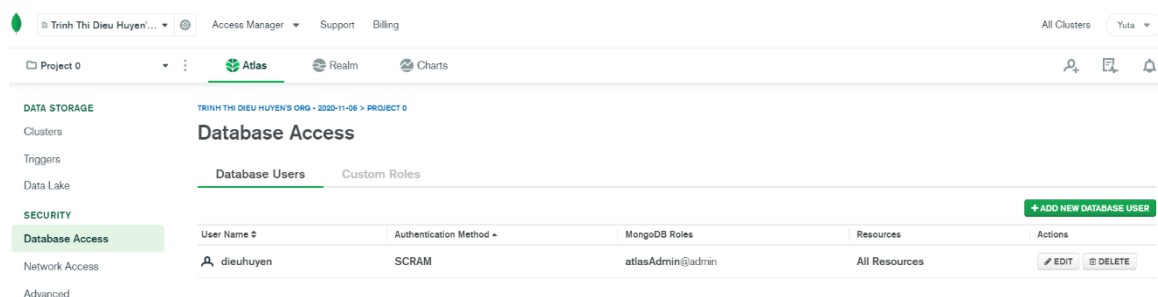


Figure 9: Configure Heroku - Step 6 - MongoDB Atlas



Figure 10: Configure Heroku - Step 7

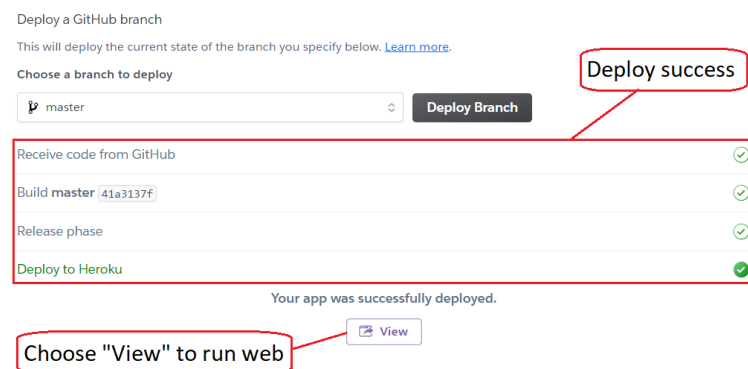


Figure 11: Configure Heroku - Step 8 – Deploy success - View your web

Below is a link leading to our website application after complete all steps above:

→ <https://huyenttdgdd18606atnselect.herokuapp.com/>

3. Images and source code for the built functions

Homepage

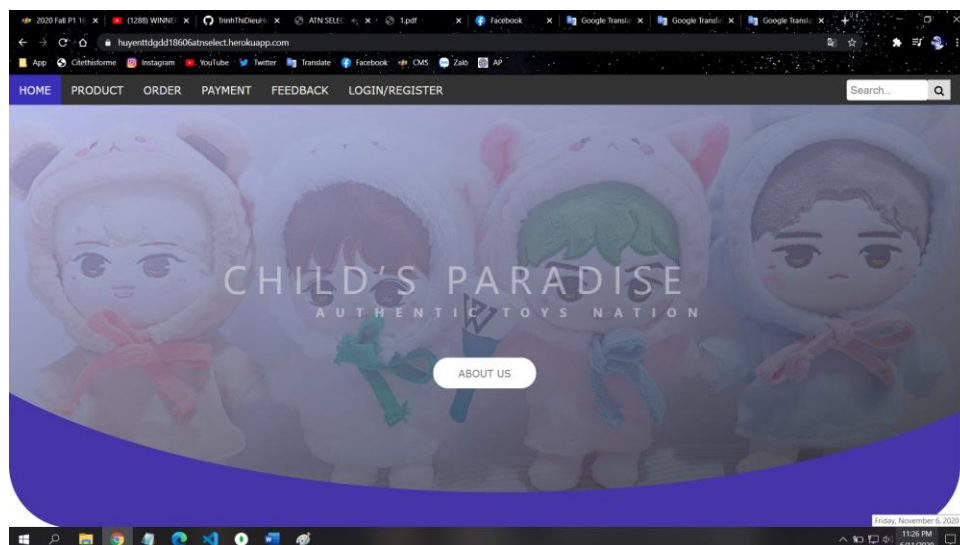


Figure 12: Homepage

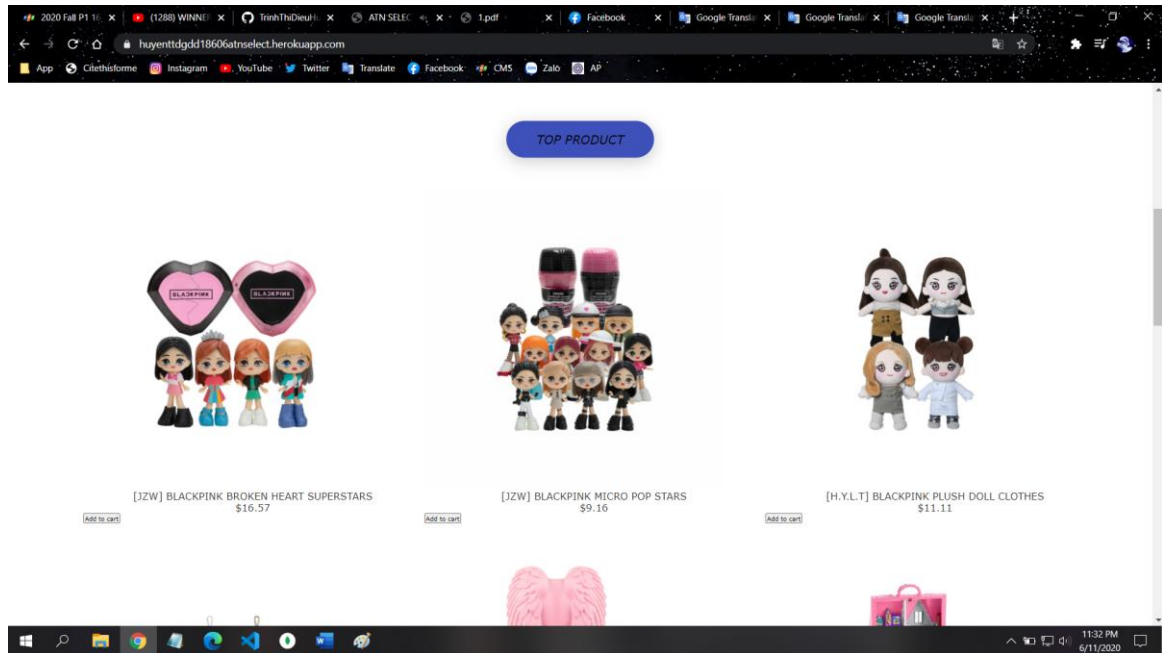


Figure 13: Homepage

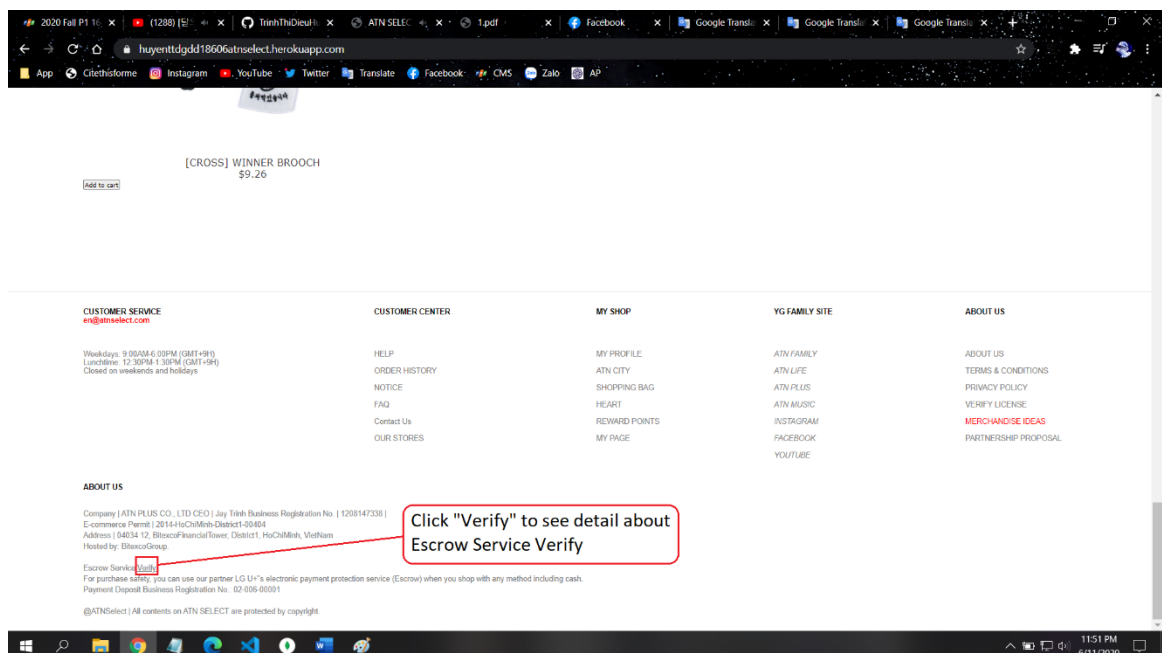


Figure 14: Homepage - Escrow Service Verify

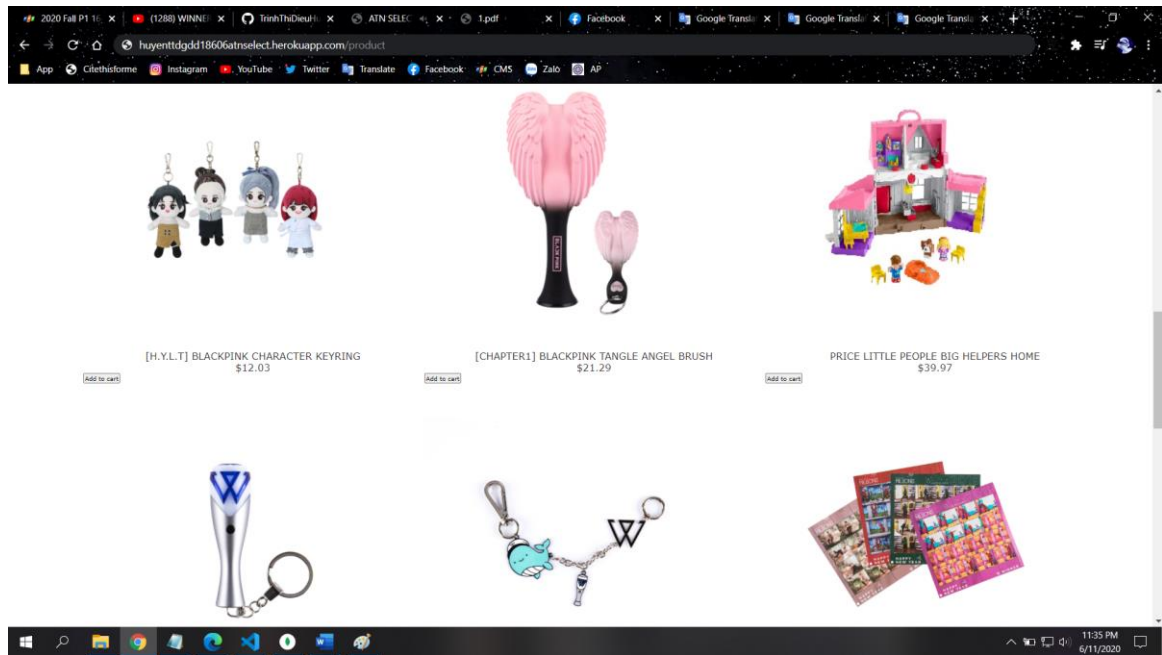


Figure 15: Product page

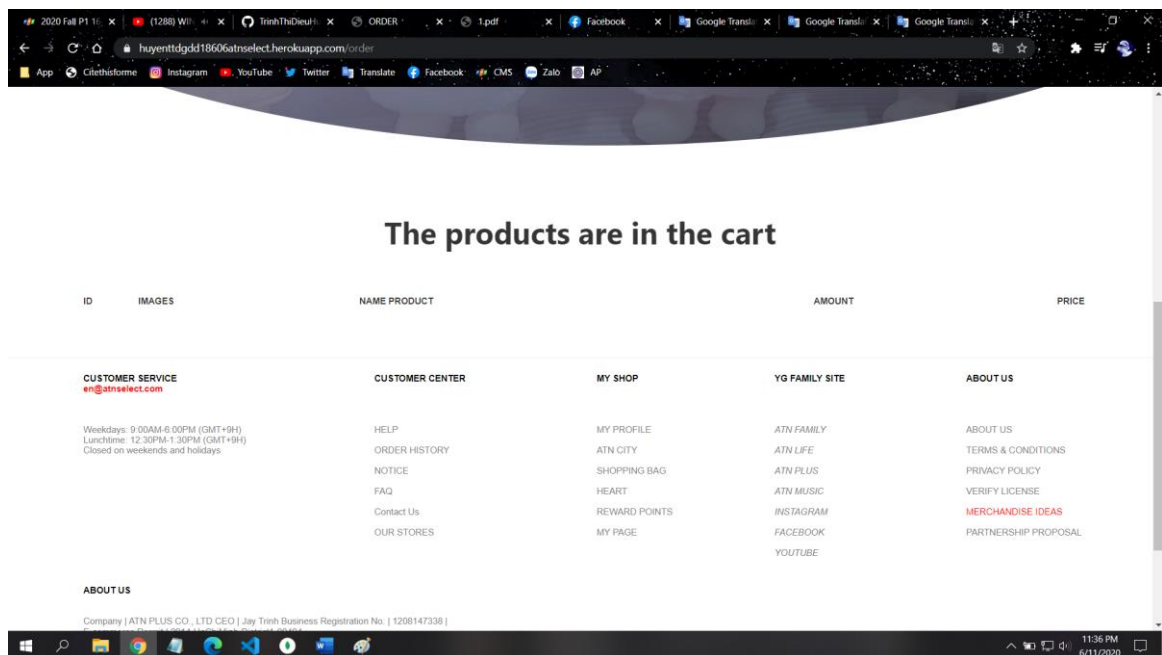


Figure 16: Order page when not yet add the product into the cart

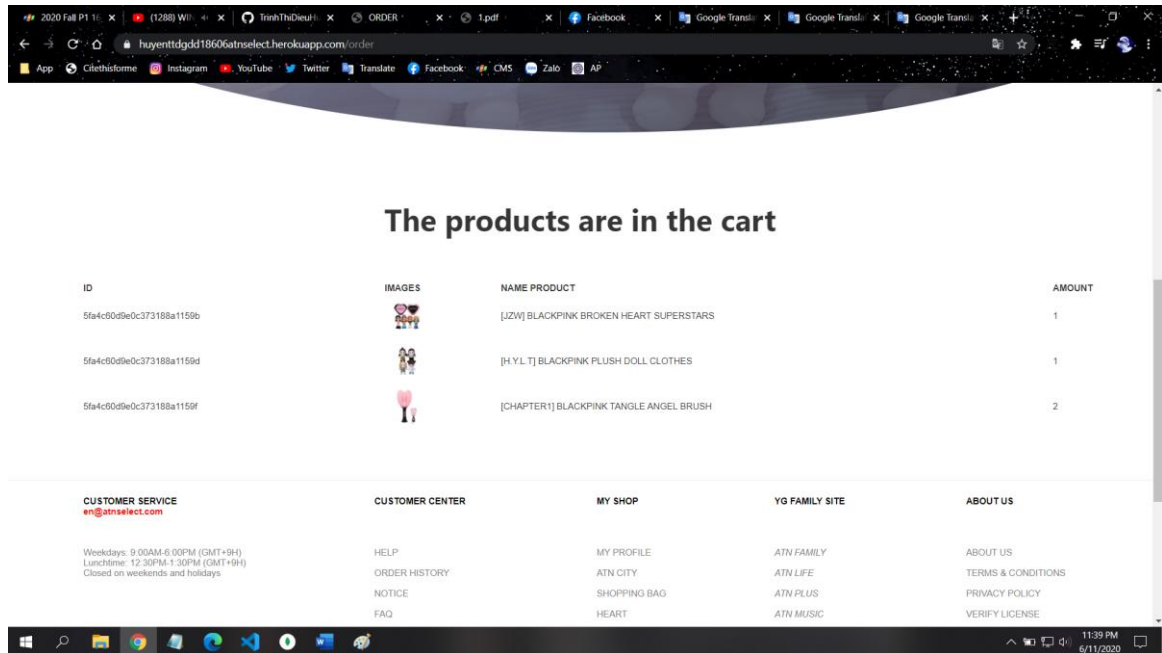


Figure 17: Order page when has added the product into the cart

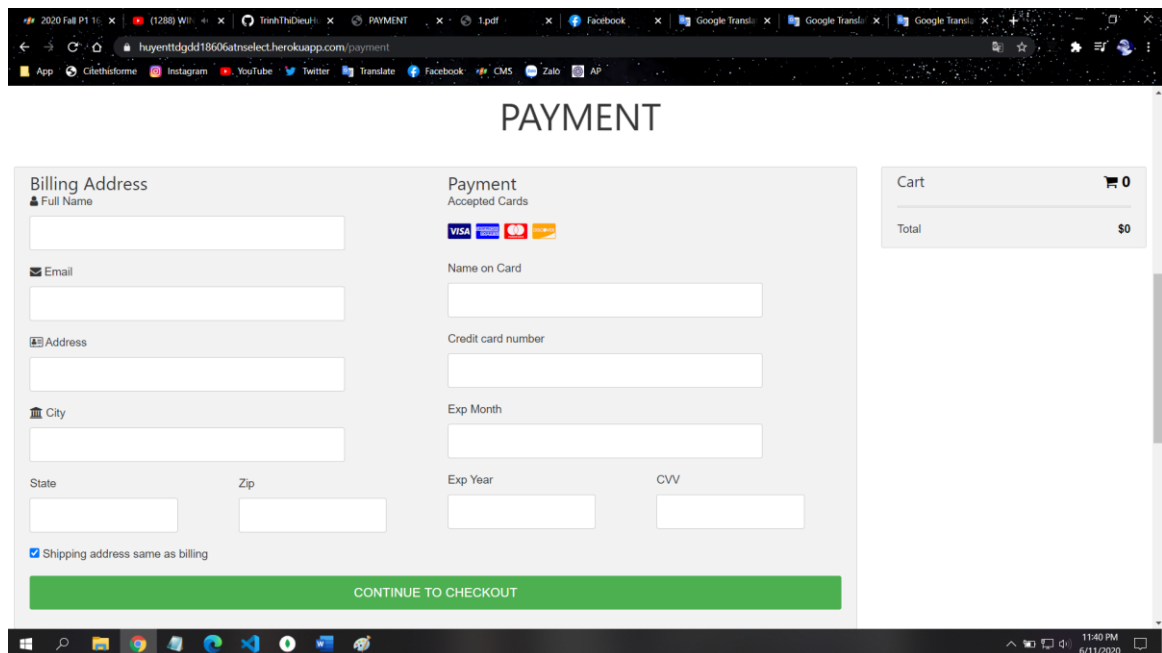


Figure 18: Payment page

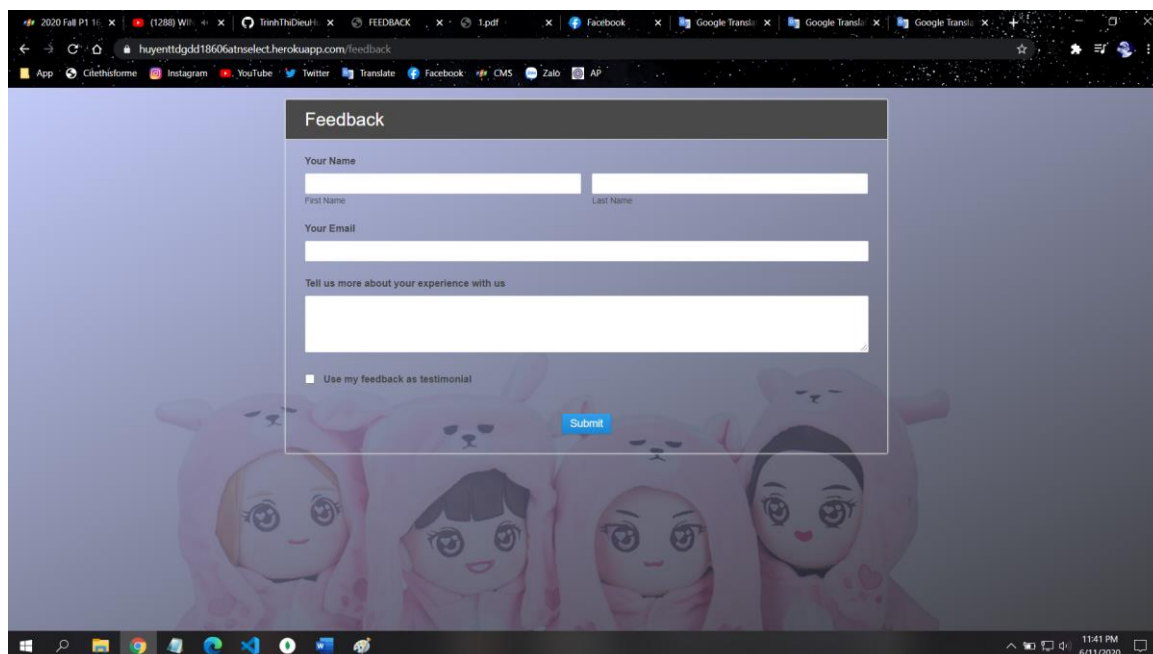


Figure 19: Feedback page

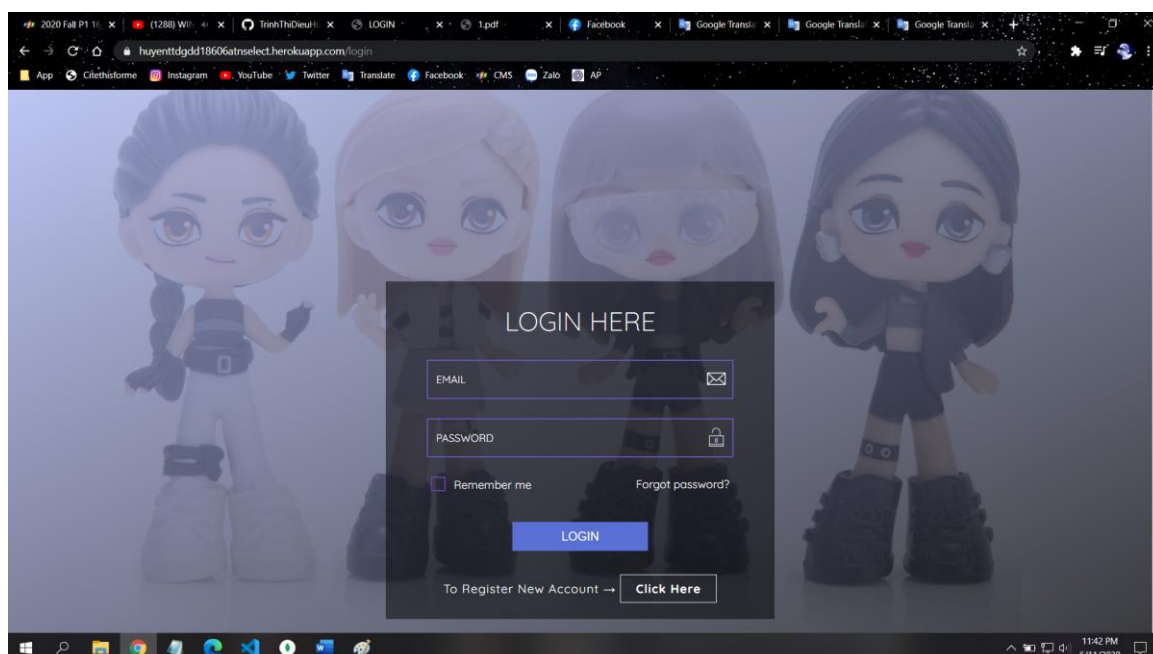


Figure 20: Login/Register page – Login form

Register Form

User Name

Email

Password

Confirm Password

☐ I Accept Terms & Conditions

Register

Figure 21: Login/Register page - Register form

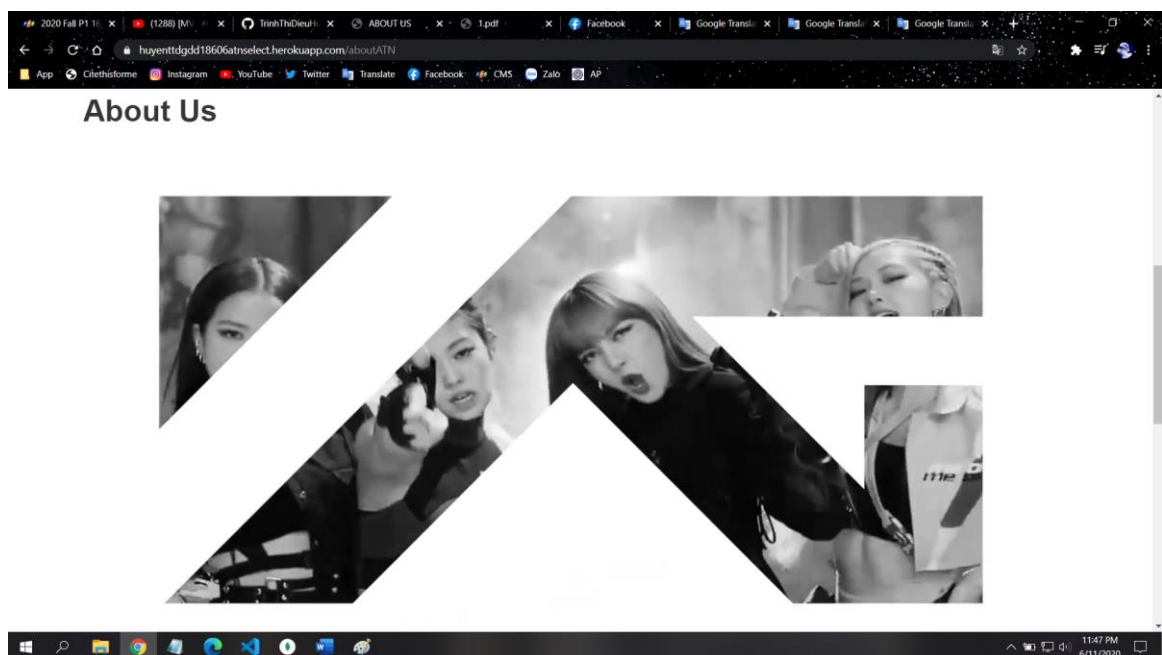


Figure 22: About ATN page

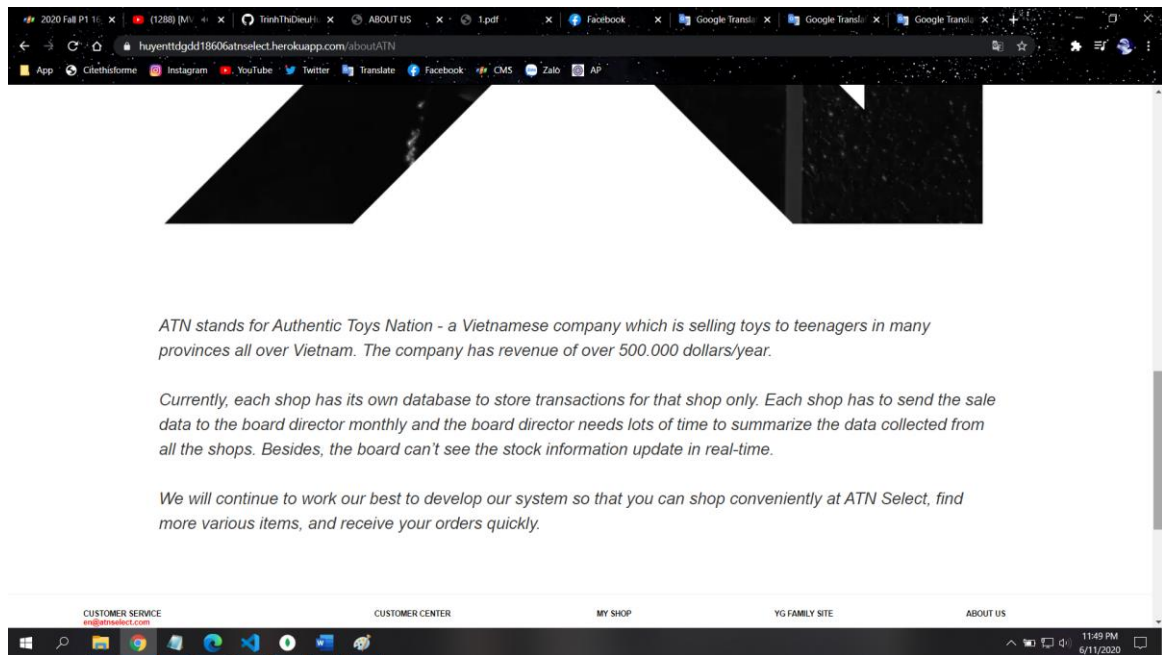


Figure 23: About ATN page

Below is a link leading to all source code for the built functions on the website application of ATN company:

→ <https://github.com/TrinhThiDieuHuyen/ATNproject.git>

4. Analysis and give possible solutions for the most common problems of a cloud computing platform

4.1. Analyze the most common problems which arise in a Cloud Computing platform and discuss appropriate solutions to these problems

Data Security, Virtualization Security, Network Security is three-issue of the most common of a cloud computing platform now.

About Data Security, due to huge infrastructure and cost organizations are slowly switching to cloud technology. Data are stored in the CSP's infrastructure. As data do not reside in organization territory, many complex challenges arise. Some of the complex data security challenges in the cloud include the following: First, the need to protect the confidential business, government, or regulatory data. Next, cloud service models with multiple tenants sharing the same infrastructure. Next, data mobility and legal issues relative to such government rule as the European Union (EU) Data Privacy Directive. Next, lack of standards about how CSPs securely recycle disk space and erase

existing data. Next, auditing, reporting, and compliance concerns. Next, loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT security intelligence and risk management. Next, a new type of insider who does not even work for your company but may have control and visibility into your data.

Such issues raise the level of anxiety about security risks in the cloud. Enterprises worry whether they can trust their employees or need to implement additional internal controls in the private cloud and whether third-party providers can provide adequate protection in multitenant environments that may also store competitor data. There is also an ongoing concern about the safety of moving data between the enterprise and the cloud, as well as how to ensure that no residual data remnants remain upon moving to another CSP. Unquestionably, virtualized environments and the private cloud involve new challenges in securing data, mixed trust levels, and the potential weakening of separation of duties and data governance. The public cloud compounds these challenges with data that are readily portable, accessible to anyone connecting with the cloud server, and replicated for availability. And with the hybrid cloud, the challenge is to protect data as it moves back and forth from the enterprise to a public cloud. However, security and privacy are still cited by many organizations as the top inhibitors of cloud services adoption, which has led to the introduction of cloud encryption systems in the past 18 months. The issues that must be addressed are as follows.

First, breach notification and data residency mean not all data require equal protection, so businesses should categorize data intended for cloud storage and identify any compliance requirements in relation to data breach notification or if data may not be stored in other jurisdictions. Gartner also recommends that enterprises should put in place an enterprise data security plan that sets out the business process for managing access requests from government law enforcement authorities. The plan should take stakeholders into accounts, such as legal, contract, and business units, security, and IT.

Next, data management at rest means businesses should ask specific questions to determine the CSP's data storage life cycle and security policy. Businesses should find out if multitenant storage is being used, and if it is, find out what separation mechanism is being used between tenants. Besides, it also means is mechanisms such as tagging are used to prevent data from being replicated to specific countries or regions. In addition, storage used for archive or backup is encrypted and the key

management strategy includes a strong identity or access management policy to restrict access within certain jurisdictions. So, Gartner recommends that businesses use encryption to implement end-of-life strategies by deleting the keys to digitally shred the data while ensuring that keys are not compromised or replicated.

Next, data protection in motion as a minimum requirement, Gartner recommends that businesses ensure that the CSP will support secure communication protocols such as Secure Socket Layer (SSL)/Transport Layer Security (TLS) for browser access or virtual private network (VPN) to based connections for system access for protected access to their services. The research note says that businesses always encrypt sensitive data in motion to the cloud, but if data are unencrypted while in use or storage, it will be incumbent on the enterprise to mitigate against data breaches. In IaaS, Gartner recommends that businesses favor CSPs that provide network separation among tenants so that one tenant cannot see another's network traffic.

About Virtualization Security, virtualization is a technology that drives server consolidation and data center operations to a key ingredient in creating a flexible, on-demand infrastructure. When adopting virtualization for cloud computing, it becomes evident that the management tools used in a physical server-based deployment will not suffice in a highly dynamic virtualized one. To begin with, in a physical server deployment model, provisioning automation is generally not as heavily used unless there is a significant enough number of server OSs to warrant doing so. Virtualization mainly focuses on three different areas are virtual networks, storage virtualization, and server virtualization.

In network virtualization, the available resources are pooled into a network and the network bandwidth is split up into multiple channels where each individual channel is independent of one another.

In storage virtualization, the combines the physical storage from multiple network storage devices, and this available storage is viewed as multiple different singular storage devices.

In server virtualization, the identity of individual server devices is masked from the users, and the servers are designed to view as individual servers where the resource sharing and maintenance complexity are managed in a balanced way.

The combination of these three virtualization components provides a self-managing capability to the resources, and this self-managing plays a major role in cloud computing. The typical strategy for provisioning physical servers involves repetitive

steps. In a heavily virtualized environment like the cloud, OS provisioning will rapidly transition to being a highly automated process. The critical areas of concern during virtualization are as follows.

First is a new threat, virtualization alters the relationship between the OS and hardware. This challenges traditional security perspectives. It undermines the comfort you might feel when you provision an OS and application on a server you can see and touch. Some already believe that this sense of comfort is misplaced in most situations. For the average user, the actual security posture of a desktop PC with an Internet connection is hard to realistically discern. Virtualization complicates the picture but does not necessarily make security better or worse. There are several important security concerns you need to address in considering the use of virtualization for cloud computing. A potential new risk has to do with the potential to compromise a VM hypervisor. If the hypervisor is vulnerable to exploitation, it will become a primary target. At the scale of the cloud, such a risk would have a broad impact if not otherwise mitigated. This requires an additional degree of network isolation and enhanced detection by security monitoring. In examining this concern, first, consider the nature of a hypervisor. It is observed that “Hypervisors are purpose-built with a small and specific set of functions. A hypervisor is smaller, more focused than a general-purpose operating system, and less exposed, having fewer or no externally accessible network ports. A hypervisor does not undergo frequent change and does not run third-party applications. The guest operating systems, which may be vulnerable, do not have direct access to the hypervisor. In fact, the hypervisor is completely transparent to network traffic with the exception of traffic to/from a dedicated hypervisor management interface.”

Second is storage concerns, it is another security concern with virtualization that has to do with the nature of allocating and deallocating resources such as local storage associated with VMs. During the deployment and operation of a VM, data are written into physical memory. If it is not cleared before those resources are reallocated to the next VM, there is a potential for exposure. These problems are certainly not unique to virtualization. They have been addressed by every commonly used OS. Not all OSs manage data clearing. Some might clear data upon resource release, others might do so upon allocation. The bottom line is to clear the data yourself, carefully handle operations against sensitive data, and pay particular attention to access and privilege controls. Another excellent security practice is to verify that a released resource was cleared. A further area of concern with virtualization has to do with the potential for undetected network attacks between VMs collocated on a physical server. Unless you

can monitor the traffic from each VM, you cannot verify that traffic is not possible between those VMs. In essence, network virtualization must deliver an appropriate network interface to the VM. That interface might be a multiplexed channel with all the switching and routing handled in the network interconnect hardware. Most fully featured hypervisors have virtual switches and firewalls that sit between the server physical interfaces and the virtual interfaces provided to the VMs.

The third is traffic management, this is another theoretical technique that might have the potential for limiting traffic flow between VMs would be to use segregation to gather and isolate different classes of VMs from each other. VMs could be traced to their owners throughout their life cycle. They would only be colocated on physical servers with other VMs that meet those same requirements for colocation. An actual practice for managing traffic flows between VMs is to use VLANs to isolate traffic between one customer's VMs and another customer's VMs. To be completely effective, however, this technique requires extending support for VLANs beyond the core switching infrastructure and down to the physical servers that host VMs. The next problem is scaling VLAN-like capabilities beyond their current limits to support larger clouds. That support will also need to be standardized to allow multivendor solutions. It will also need to be tied in with network management and hypervisors.

About Network Security, the cloud is based on the networking of many things together like the network of infrastructure. While the network is the backbone of the cloud, many challenges are encountered in this network. Some of the challenges in the existing cloud networks are discussed in the following.

First is application performance, cloud tenants should be able to specify bandwidth requirements for applications hosted in the cloud, ensuring similar performance to on-premise deployments. Many tiered applications require some guaranteed bandwidth between server instances to satisfy user transactions within an acceptable time frame and meet predefined service-level agreements (SLAs). Insufficient bandwidth between these servers will impose significant latency on user interactions. Therefore, without explicit control, variations in cloud workloads and oversubscription can cause delay and drift of response time beyond acceptable limits, leading to SLA violations for the hosted applications.

Next is the flexible deployment of appliances, enterprises deploy a wide variety of security appliances in their data centers, such as deep packet inspection (DPI) or intrusion detection systems (IDSs), and firewalls to protect their applications from attacks. These are often employed alongside other appliances that perform load

balancing, caching and application acceleration. When deployed in the cloud, an enterprise application should continue to be able to flexibly exploit the functionality of these appliances.

Next is the policy enforcement complexities, traffic isolation, and access control to end users are among the multiple forwarding policies that should be enforced. These policies directly impact the configuration of each router and switch. Changing requirements, different protocols (e.g., Open Shortest Path First [OSPF], LAG (Link Aggregation Group), Virtual Router Redundancy Protocol [VRRP]), and different flavors of L2 spanning tree protocols, along with vendor-specific protocols, make it extremely challenging to build, operate, and interconnect a cloud network at scale.

Next is the topology-dependent complexity, the network topology of data centers is usually tuned to match a predefined traffic requirement. For instance, a network topology optimized for east-west traffic (i.e., traffic among servers in a data center) is not the same as a topology for north-south (traffic to/from the Internet). The topology design also depends on how L2 and/or L3 is utilizing the effective network capacity. For instance, adding a simple link and switch in the presence of a spanning tree-based L2 forwarding protocol may not provide additional capacity. Furthermore, evolving the topology based on traffic pattern changes also requires a complex configuration of L2 and L3 forwarding rules.

Next is the application rewriting, applications should run out of the box as much as possible, in particular for IP addresses and network-dependent failover mechanisms. Applications may need to be rewritten or reconfigured before deployment in the cloud to address several network-related limitations. Two key issues are (1) lack of a broadcast domain abstraction in the cloud network and (2) cloud-assigned IP addresses for virtual servers.

Next is the location dependency, network appliances, and servers (e.g., hypervisors) are typically tied to a statically configured physical network, which implicitly creates a location-dependent constraint. For instance, the IP address of a server is typically determined based on the VLAN or the subnet to which it belongs. VLANs and subnets are based on the physical switch port configuration. Therefore, a VM cannot be easily and smoothly migrated across the network. Constrained VM migration decreases the level of resource utilization and flexibility. Besides, physical mapping of VLAN or subnet space to the physical ports of a switch often leads to a fragmented IP address pool.

Finally is the multilayer network complexity, a typical three-layer data center network includes a TOR (Top of Rack) layer connecting the servers in a rack, an aggregation layer, and a core layer, which provides connectivity to/from the Internet edge. This multilayer architecture imposes significant complexities in defining boundaries of L2 domains, L3 forwarding networks and policies, and layer-specific multivendor networking equipment. Providers of cloud computing services are currently operating their own data centers. Connectivity between the data centers to provide the vision of one cloud is completely within the control of the CSP. There may be situations where an organization or enterprise needs to be able to work with multiple cloud providers due to locality of access, migration from one cloud service to another, the merger of companies working with different cloud providers, cloud providers who provide the best-of-class services, and similar cases. Cloud interoperability and the ability to share various types of information between clouds become important in such scenarios. Although CSPs might see the less immediate need for any interoperability, enterprise customers will see a need to push them in this direction. This broad area of cloud interoperability is sometimes known as cloud federation.

4.2. Discuss the issues and constraints one can face during the development process

Cloud computing is slowly gaining acceptance within businesses. It is predicted that by 2018, 59% of the cloud workload will be generated from Software-as-a-Service (SaaS). According to a recent survey, 43% of IT decision-makers are planning to invest more in cloud computing. Cloud's popularity has grown immensely, as more and more recognize its benefits of improving data access, freeing up IT resources for more strategic tasks, cutting and increasing flexibility and efficiency. The usage of cloud services has become closely associated with common cloud offerings, such as Software as a service (SaaS), Platform as service (PaaS), and Infrastructure as a service (IaaS).

First are privacy and security, cloud architecture does not automatically grant security compliance for the end-user data or apps on them, so apps written for cloud have to be secure on their own terms. Some of the responsibility for this does fall to cloud vendors, but the lion's share of it is still in the lap of the application designers. Cloud computing introduces another level of risk because essential services are often outsourced to a third party, making it harder to maintain data integrity and privacy.

Next is client incomprehension, we have probably passed the days when people thought cloud was just big server clusters, but that doesn't mean that we can ignore

the fact about a cloud moving forward. There are also too many misunderstandings about how public and private clouds work together, misunderstandings about how easy it is to move from one kind of infrastructure to another. A good way to combat this is to prevent customers from real-world examples of what is possible and why so that they can base their understanding on the actual working.

Next is data security, a of the major concerns associated with cloud computing is its dependency on the cloud service provider. For uninterrupted and fast cloud service you need to choose a vendor with proper infrastructure and technical expertise. Since you would be running your company's asset and data from a third-party interface ensuring data security and privacy are of utmost importance. Hence, when engaging a cloud service provider, always inquire about their cloud-based security policies. However, cloud service companies usually employ strict data security policies to prevent hacking and invest heavily in improved infrastructure and software.

Next is addressing growing integration complexities, many applications have complex integration needs to connect to applications on the cloud network, as well as to other on-premises applications. These include integrating existing cloud services with existing enterprise applications and data structures. There is a need to connect the cloud application with the rest of the enterprise in a simple, quick, and cost-effective way. Integrating new applications with existing ones is a significant part of the process and cloud services bring even more challenges from an integration perspective.

Next are reliability and availability, cloud service providers still lack round-the-clock service, this result in frequent outages. It is important to monitor the service being provided using internal or third-party tools. It is vital to have plans to supervise usage, performance, and business dependency of these cloud services.

Next are performance and bandwidth cost, businesses can save money on hardware but they have to spend more on the bandwidth. This could be a low cost for small applications but can be significantly high for data-intensive applications. Delivering intensive and complex data over the network requires sufficient bandwidth. Because of this many enterprises are waiting for a reduced cost, before switching to cloud services.

Next is selecting the right cloud set-up, there are three types of cloud environments available (private, public, and hybrid). The secret of successful cloud implementation lies in choosing the most appropriate cloud set-up. Big companies feel safer with their vast data in private cloud environments, small enterprises often benefit economically by hosting their services in the public cloud. Some companies also prefer the hybrid

cloud because it is flexible, cost-effective, and offers a mix of public and private cloud services.

Next is the dependency on service providers, one of the major issues with cloud computing is its dependency on the service provider. The companies providing cloud services charge businesses for utilizing cloud computing services based on usage. Customers typically subscribe to cloud services to avail of their services. For uninterrupted and fast services one needs to choose a vendor with proper infrastructure and technical expertise. You need a vendor who can meet the necessary standards. The service-level agreement should be read carefully and understood in detail in case of an outage, lock-in-clauses, etc. Cloud service is any service made available to businesses or corporates from a cloud computing provider's server. In other words, cloud services are professional services that support organizations in selecting, deploying, and managing various cloud-based resources.

Finally is seeing beyond the challenges, these challenges should not be considered as roadblocks in the pursuit of cloud computing. It is rather important to give serious considerations to these issues and the possible ways out before adopting the technology. Cloud computing is rapidly gaining enterprise adoption, yet many IT professionals still remain skeptical, for good reason. Issues like security and standards continue to challenge this emerging technology. Strong technical skills will be essential to address the security and integration issues in the long run. There are also issues faced while making transitions from the on-premise set-up to the cloud services like data migration issues and network configuration issues. But planning ahead can avoid most of these problems with cloud configurations. The extent of the advantages and disadvantages of cloud services vary from business to business, so it is important for any business to weigh these up when considering their move into cloud computing.

4.3. Critically discuss how one can overcome these issues and constraints

Have ten challenge are optimizing cloud expenses, working with poly cloud environments, migrating existing applications onto the cloud, adapting the cloud-first model, cost calculations within limits, converting back office activities, meeting governing compliance, proprietary lock-in, consistent performance, and data security violation.

About optimizing cloud expenses, this has been one of the most challenging tasks for cloud users. A tad more than security issues, managing cloud spending is a tough task.

With multiple reasons involved, organizations tend to waste quite a lot of their budget in unnecessary activities involved through the cloud. Be it carelessness, lack of knowledge, hurried operations, unskilled resources, what happens is that the costs associated with cloud computing go beyond limits. You can overcome the challenge by seeking assistance from various technological solutions for cloud cost management, involving a cloud computing partner who is skilled and experience at cloud solution management or creating a centralized cloud team to look at the budget details.

About working with poly cloud environments, with increasing options in cloud solutions, most enterprises are moving towards the multi-cloud model of working. This strategy brings along with multiple cloud types as well as multiple cloud vendors involved. That itself poses as a challenge to manage the synchronization, security, and robustness of operations within the organization as well as with multiple cloud service providers. You can overcome the challenge by adapting best practices such as performing research and training, dynamically managing vendor relationships, redesigning processes to involve all stakeholders and cloud patterns, integrating cloud solutions by various service providers into one, and managing or maintaining a proper infrastructure to encompass the entire functioning.

About migrating existing applications onto the cloud, you compare developing a totally new cloud application as against migrating an existing application onto the cloud, the answer is straight and simple. Migrating an existing one has its own set of hurdles, drawbacks, and challenges to face. Time has proven that cloud migration has faced troubles like security configuration, time consumption, budget overflow, unmatched requirements, downtime, etc. You can overcome the challenge by performing pre-migration testing that focuses primarily on migration-related needs, setting a realistic project deadline or budget keeping in mind migration hassles, and hiring cloud service providers who are experts at migration projects

About adapting the cloud-first model, there are many enterprises who aren't yet prepared to embrace the cloud culture but are still rushing onto doing it, because of peer competition in the market. It strikes as an awkward position for such organizations who do not understand the complete significance of the cloud and have half knowledge of how exactly the cloud would help their business. They are not able to understand the changes in operations, infrastructure, and environment that would be present with cloud computing solutions. You can overcome the challenge by training organizations with much-needed knowledge about the cloud, appraising

teams about what is in store for them after cloud implementation, and showing them live success stories that have benefited out of cloud implementations.

About cost calculations within limits, because cloud operations are comparatively new, organizations do not tend to budget their expenses properly. Operational costs may differ enterprise to enterprise and the budget may fluctuate. There could be some unseen expenses that may tend to change the budget limits and cross over. Even small businesses find it difficult to execute cloud solutions within the stipulated budget. You can overcome the challenge by preparing a cost estimate plan right from the beginning, involving cost experts who can foresee all included expenditure, and keeping aside a section of the budget for unseen situations

About converting back office activities, it is easy for the development culture to migrate to the cloud along with their technological advancements. As for the backend processes like accounting and billing systems have a tough task with the changeover since they will be migrating more towards a subscription-oriented solution. This could hamper team reimbursement, attendance data, etc. You can overcome the challenge by maintaining all necessary employee information in the cloud right from the beginning, and having a detailed approach to migrate accounting and finance details to the cloud.

About meeting governing compliance, since the cloud offers benefits in bulk, they are always in demand, and more so is the data processing across cloud solutions. The prime concern, therefore, is the security of the information that is being processed. Safeguarding this data is the responsibility of the cloud service provider as well as the client. Abiding by rules and regulations is very vital to ensure the accuracy and security of information flow in the cloud. You can overcome the challenge by designing compliance protocols in security frameworks, being more focused on data circulation or relevant protection, and implementing a cloud management solution that adheres to regulatory compliance for utmost data protection.

About proprietary lock-in, vendor lock-in, or proprietary lock-in is a case in which the client using a product cannot simply transition to a peer product. It is basically due to technologies or other standards that are incompatible with each other. This is what happens with vendors in cloud computing. For IT leaders, global giants like AWS, Microsoft Azure, GCP may cause a threat of vendor lock-in. You can overcome the challenge by being careful while purchasing cloud facilities from multiple cloud service providers, assuring from the start that the services involved are compatible with other providers, and understanding the requirements from all ends.

About consistent performance, in the case of mission-critical solutions, performance plays a pivotal role in cloud-based applications. That is because any downtime on the cloud directly hampers the performance of the application. Cloud downtime could be possible in any technology. After all, no cloud service is full proof. At such times, it becomes difficult for the client to survive the mission-critical application. You can overcome the challenge by creating comprehensive application recovery solutions for the cloud-based data, having proper disaster recovery mechanisms in place, and offer failover mechanisms by third-party vendors in case of downtime.

About data security violations, it was and is a matter of concern for cloud computing. Data security has always been on the top list of challenges, especially when it comes to cloud-based services. With a variety of industry segments adapting to the cloud culture, data violation can create havoc for end-users. Be it public, private, or hybrid, be it poly cloud or single cloud, lack of security measures can directly hamper the working of the organization. You can overcome the challenge by having a tight security protection protocol for the cloud solution, evolving corporate culture that ensures data security, and training and certifying IT staff to handle security issues with an appropriate solution.

5. Analysis and discussion on how to overcome of the most common security issues in the cloud environment

1.1. Assess the most common security issues in cloud environments

Have four of the most common security issues in cloud environments need assess are software-as-a-service security issues, platform-as-a-service security issues, infrastructure-as-a-service security issues, and audit/compliance issues.

About software-as-a-service security issues, in a traditional on-premise application deployment model, the sensitive data of each enterprise continue to reside within the enterprise boundary and are subject to its physical, logical, and personnel security and access control policies. The architecture of SaaS based applications is specifically designed to support many users concurrently (multitenancy). SaaS applications are accessed through the web, and so web browser security is very much important. Information security officers will need to consider various methods of securing SaaS applications. Web services (WS) security, Extensible Markup Language (XML) encryption, SSL, and available options used in enforcing data protection transmitted over the Internet. In the SaaS model, the enterprise data are stored outside the enterprise boundary, at the SaaS vendor end. Consequently, the SaaS vendor must

adopt additional security checks to ensure data security and to prevent breaches due to security vulnerabilities in the application or through malicious employees. This involves the use of strong encryption techniques for data security and fine grained authorization to control access to data. Below is the pain points of concern in SaaS.

First is network security, in an SaaS deployment model, sensitive data flow over the network needs to be secured in order to prevent leakage of sensitive information. This involves the use of strong network traffic encryption techniques such as the SSL and TLS for security.

Second is resource locality, in an SaaS model of a cloud environment then the end users use the services provided by the cloud providers without knowing exactly where the resources for such services are located. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in much enterprise architecture. The directive prohibits transfers of personal data to countries that do not ensure an adequate level of protection. For example, the recent Dropbox users have to agree to the Terms of Service that grant the providers the right to disclose user information in compliance with laws and law enforcement requests.

Third is cloud standards, to achieve interoperability among clouds and to increase their stability and security, cloud standards are needed across organizations. For example, the current storage services by a cloud provider may be incompatible with those of other providers. In order to keep their customers, cloud providers may introduce so called sticky services that create difficulty for the users if they want to migrate from one provider to the other.

Fourth is data segregation, multitenancy is one of the major characteristics of cloud computing. In a multitenancy situation, data of various users will reside at the same location. Intrusion of data of one user by another becomes possible in this environment. This intrusion can be done either by hacking through the loop holes in the application or by injecting client code into the SaaS system. An SaaS model should, therefore, ensure a clear boundary for each user's data. The boundary must be ensured not only at the physical level but also at the application level. The service should be intelligent enough to segregate the data from different users.

Fifth is data access, data access issue is mainly related to security policies provided to the users while accessing the data. The organizations will have their own security policies based on which each employee can have access to a particular set of data. The security policies may entitle some considerations, wherein some of the employees are not given access to a certain amount of data. These security policies must be adhered

by the cloud to avoid intrusion of data by unauthorized users. The SaaS model must be flexible enough to incorporate the specific policies put forward by the organization. The model must also be able to provide organizational boundary within the cloud because multiple organizations will be deploying their business processes within a single cloud environment.

Sixth is data breaches, since data from various users and business organizations lie together in a cloud environment, breaching into the cloud environment will potentially attack the data of all the users. Thus, the cloud becomes a high value target.

Seventh is backup, the SaaS vendor needs to ensure that all sensitive enterprise data are regularly backed up to facilitate quick recovery in case of disasters. Also, the use of strong encryption schemes to protect the backup data is recommended to prevent accidental leakage of sensitive information. In the case of cloud vendors such as Amazon, the data at rest in S3 are not encrypted by default. The users need to separately encrypt their data and backups so that it can't be accessed or tampered with by unauthorized parties.

Eighth is identity management (IdM) and sign on process, IdM deals with identifying individuals in a system and controlling the access to the resources in that system by placing restrictions on the established identities. When an SaaS provider has to know how to control who has access to what systems within the enterprise, it becomes all the more challenging task. In such scenarios, the provisioning and deprovisioning of the users in the cloud become very crucial.

About platform-as-a-service security issues, PaaS provides a ready to use platform, including OS that runs on vendor provided infrastructure. As the infrastructure is of the CSP, various security challenges of the focused architecture are caused mainly by the spread of the user objects over the hosts of the cloud. Stringently allowing access of objects to the resources and defending the objects against malicious or corrupt providers reasonably reduce possible risks. Network access and service measurement bring together concerns about secure communications and access control. Well known practices, object scale enforcement of authorization, and undeniable traceability methods may alleviate the concerns. Apart from the aforementioned problems, user privacy must be protected in a public, shared cloud. Therefore, proposed solutions must be privacy aware. Service continuity is another concern for many enterprises that consider cloud adoption. Accordingly, fault tolerant reliable systems are required.

About infrastructure-as-a-service security issues, cloud computing makes a lot of promises in the areas of increased flexibility and agility, potential cost savings, and competitive advantages for developers so that they can stand up an infrastructure quickly and efficiently to enable them to develop the software to drive business success. There are a lot of problems that cloud, especially private cloud, solves, but it is not that much good in solving problems related to security. However, in a private cloud environment, some of the traditional problems faced include hypervisor security, multitenancy, identity management and access control (IdAM), and finally network security.

First is hypervisor security, in the private cloud than most or all of the services will run in a virtualized environment and the security model used by the hypervisor cannot be taken for granted. A need to evaluate the security models and the development of hypervisors becomes necessary.

Next is multitenancy, although all the tenants in the multitenancy environment will be from the same company, not all tenants may be comfortable sharing infrastructure with other users within the same company.

Next are identity management and access control (IdAM), in a traditional data center, we were comfortable with the small handful of authentication repositories we had to work with Active Directory being one of the most popular. But with private cloud, handling authentication and authorization for the cloud infrastructure, handling tenants, and handling delegation of administration of various aspects of the cloud fabric are the major tasks to be addressed.

Next is network security, in the private cloud, we are likely to have many components of a service communicate with each other over virtual network channels only. Assessing the traffic, employing some powerful access controls for physical networks, and control quality of service, which is a key issue in the availability aspect of the confidentiality, integrity, and availability (CIA) security model are major concerns.

As a consolidation, platform-related security considers the previously said three service delivery models like SaaS, PaaS, and IaaS, and the concerned components are also mentioned individually. Combining the three types of clouds (public cloud, private cloud, and hybrid cloud) together with the three service delivery models, we get a complete picture of a cloud computing environment interlinked by connectivity devices coupled with information security components. Virtualized physical resources, virtualized infrastructure, virtualized middleware platforms, and business-related applications are being provided as computing services in the cloud. Cloud providers

and cloud consumers must be able to maintain and establish computing security at all levels of interfaces in the cloud computing architecture.

Regarding audit and compliance, it is a widely known fact that data protection and regulatory compliance are among the top security concerns for chief information officers (CIOs) of any organization. According to the 'Pew Internet and American Life Project', an overwhelming majority of users of cloud computing services expressed serious concern about the possibility of a service provider disclosing their data to others. Ninety per- cent of cloud application users said that they would be very concerned if the company at which their data were stored sold them to another party. A survey conducted by many firms expressed the view that security is the biggest challenge for the cloud computing model. Stakeholders, therefore, increasingly feel the need to prevent data breaches. In recent months, many newspaper articles have revealed data leaks in sensitive areas such as the financial and governmental domains and web communities.

One of the missions of the data protection authorities is to prevent the so-called Big Brother phenomenon, which refers to a scenario whereby a public authority processes personal data without adequate privacy protection. In such a situation, end-users may view the cloud as a vehicle for drifting into a totalitarian surveillance society. The specificities of cloud computing, therefore, make the data protection incentive even greater. For example, the cloud provider should provide encryption to protect the stored personal data against unauthorized access, copy, leakage, or processing. In a cloud environment, companies have no control over their data, which, being entrusted to third-party application service providers in the cloud, could now reside anywhere in the world. Nor will a company know in which country its data reside at any given point in time. This is a central issue of cloud computing that conflicts with the EU requirements whereby a company must at all times know where the personal data in its possession are being transferred to. Cloud computing thus poses special problems for multinationals with specific EU customers.

1.2. Discuss how to overcome these security issues when building a secure cloud platform

While there is always some risk to any IT environment, there are some things that can be done to minimize, if not eliminate many of the issues outlined above, such as limit your cloud computing vendors, verify your access to information about the cloud environment, verify security SLAs, check for specific security measures, and consult with a cybersecurity expert.

About limit your cloud computing vendors, one of the major challenges in dealing with cloud-based solutions is that they can all have different security tools and processes, which makes them more difficult to manage. Finding ways to limit your selection of CSP vendors can be a major help. When possible, consider sourcing as many cloud solutions from a single vendor as you can. However, this is often easier said than done.

About verify your access to information about the cloud environment, because visibility is so important to cybersecurity, it's important to verify what information about the cloud environment you will have access to preferably before signing an agreement. With greater visibility into the cloud environment, you can more easily track and control security.

About verify security SLAs, another thing to check before signing an agreement with a cloud service provider is what their service level agreements are regarding security. How quickly will they resolve a security breach after detection? How long will it take to restore normal service? Who is responsible for notifying affected parties? Verifying these SLAs prior to signing an agreement can help ensure that they meet your industry's cybersecurity standards, it also will protect your business from untenably long service disruptions, and establish who is responsible for what following a data breach.

About check for specific security measures, how will the CSP ensure that attackers don't infiltrate your cloud environment? How will they limit the spread of attacks from one node on their network to another? Checking what security measures a cloud service provider has to offer is crucial for establishing how prepared they are to protect your information, their ability to meet compliance standards, and how easy or difficult it will be to incorporate the solution into your existing cybersecurity architecture. Besides, note that not all cloud solutions will provide built-in security for the cloud computing environment. PaaS and IaaS solutions, in particular, will likely leave it up to their customers to incorporate the appropriate security systems to protect the cloud environment

About consult with a cybersecurity expert, when in doubt then get help. If you are ever unsure of whether a cloud solution has the right security measures to protect your organization's data, employees, and clients, consult with a cybersecurity expert. Having a bit of expert advice can help you make a more informed decision that will help you protect your organization better in the long term.

1.3. Critically discuss how an organization should protect their data when they migrate to a cloud solution

Now we will critically discuss how an organization should protect their data when they migrate to a cloud solution. First is know your data, mean really know what is happening now before you move the data. Think about the analogy of doing a house cleaning and organizing what you own before putting things in storage to sell your house. If you don't want to catalog everything then that is which is a mistake, at least know where the most important data is. Who is doing what regarding the cloud already? What data is sensitive? This is your as-is data inventory situation with known protections of current data and doesn't forget to shadow IT because there are plenty of vendor organizations that can help you through this process. On the other hand, need to define and enforce the data life cycle policy. You need to know what data is being collected by your business processes, where does it go, who is accountable (now) and what policies are in force. Can put ask that, is there appropriate training happening now? Is it working? What policies are in place to govern the movement of your data?

Next, need to know your cloud options are private, public, hybrid, or community cloud? This simple step often gets confusing, in my experience, because some staff mixes these terms up with the "public sector" and "private sector" definitions wrongly thinking that a private cloud means private-sector-owned cloud. We will repeat some basic concepts for each type of cloud. Private Cloud - the organization can have its own cloud where resource pooling is done by the organization itself. May be or may not be on-premises in your own data centers. Public Cloud - different tenants are doing resource pooling among the same infrastructure. It can be easily consumable, and the consumer can provide the resource. However, consumers will not get the same level of isolation as a private cloud. Community cloud - sharing the cloud with different organizations usually unified by the same community sharing underlined infrastructure halfway between private and public small organizations pooling resources among others. For example, some state and local government organizations share email hosting with other state and local governments in the U.S only. Hybrid cloud - a mixture of both private and public i.e., some organizations might say we would like elasticity and cost-effectiveness of public cloud and we want to put certain applications in the private cloud.

Next, must understand and clearly articulate your Identity and Access Management (IAM) roles responsibilities, and demarcation points for your data. Who owns the

data? Who are the custodians? Who has access? Who can add, delete, or modify the data? Really not just on paper? How will this change with your cloud provider? On the other hand, also need to build a system administration list. Insist on rigorous compliance certifications incorporate appropriate IAM. Mean, incorporate appropriate IAM from the outset, ideally based on roles, especially for administration duties. When you move to the cloud, the customers, not the provider, are responsible for defining who can do what within their cloud environments. Your compliance requirements will likely dictate what your future architecture in the cloud will look like. Note that these staff may need background checks, a process to update lists for new employees and staff that leave, and segregation of duties as defined by your auditors. Besides, should apply encryption thinking end to end data at rest and data in transit. We could do an entirely separate blog on this encryption topic since a recent and scary is report says there is no encryption on 82 percent of public cloud databases. Have is a few points to consider are who controls and has access to the encryption keys? What data is truly being encrypted and when? Only sensitive data? All data?

Next is to test your controls, once you move the data then your cloud solution vulnerability testing should be rigorous and ongoing and include penetration testing. Have a question put is how do you truly know your data is safe? What tools do you have to see your data in the cloud environment? How transparent is this ongoing process? The cloud service provider should employ industry-leading vulnerability and incident response tools. For example, solutions from these incidence response tools enable fully automated security assessments that can test for system weaknesses and dramatically shorten the time between critical security audits from yearly or quarterly, to monthly, weekly, or even daily. You can decide how often a vulnerability assessment is required, varying from device to device and from network to network. Scans can be scheduled or performed on demand.

Finally is back up all data in a distinct fault domain. Gartner recommends: “To spread risk most effectively, back up all data in a fault domain distinct from where it resides in production. Some cloud providers offer backup capabilities as an extra cost option, but it isn’t a substitute for proper backups. Customers, not cloud providers, are responsible for determining appropriate replication strategies, as well as maintaining backups.”

6. Summary

We implemented and completed almost all requirements base on the scenario and architecture design in the first assignment provides the implementation. However,

because of the time constraint of the assignment, the implementation just provides some demo functions of the scenario. We showed which functions are implemented, how to config, deploy, and test the services (Web application, Database Server, Source code management, server logs..) using the service provider's frameworks and open source tools. In addition, we also showed images for the built functions and give the link leading to the source code for the built application and the link leading to the website ATN company. On the other hand, we analyzed the most common problems of a cloud computing platform and given possible solutions to these problems. Besides, we also analyzed the most common security issues in the cloud environment and discussion on how to overcome these issues.

References

- [1] C. Surianarayanan and P. Chelliah, n.d, 2015. *Essentials Of Cloud Computing*. Available at: <https://www.researchgate.net/publication/257883293_An_analysis_of_security_issues_for_cloud_computing> [Accessed 5 November 2020].
- [2] Andrew Larkin, 2019. *Disadvantages Of Cloud Computing - Cloud Academy Blog*. [online] Cloud Academy. Available at: <<https://cloudacademy.com/blog/disadvantages-of-cloud-computing/>> [Accessed 5 November 2020].
- [3] K. Hashizume, D.G. Rosado, E. Fernández-Medina, et.al, 2013. *An Analysis Of Security Issues For Cloud Computing*. [ebook] Available at: <<https://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5#citeas>> [Accessed 5 November 2020].
- [4] Dina Destreza, 2017. *Challenges Of Cloud Service Development*. [online] Business 2 Community. Available at: <<https://www.business2community.com/cloud-computing/challenges-cloud-service-development-01786930>> [Accessed 5 November 2020].
- [5] Admin, 2020. *Security Issues In Cloud Computing | McAfee*. [online] McAfee.com. Available at: <<https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/security-issues-in-cloud-computing.html>> [Accessed 5 November 2020].
- [6] Admin, 2020. [online] Available at: <<https://www.business2community.com/cloud-computing/challenges-cloud-service-development-01786930>> [Accessed 26 October 2020].
- [7] Dosal, E., 2020. *How To Overcome Cloud Security Challenges [+ Solutions]*. [online] Compuquip.com. Available at: <<https://www.compuquip.com/blog/cloud-computing-security-challenges-and-solutions>> [Accessed 6 November 2020].

- [8] Lohrmann, D., 2020. 7 Tips For Securely Moving Data To The Cloud. [online] Govtech.com. Available at: <<https://www.govtech.com/blogs/lohrmann-on-cybersecurity/7-tips-for-securely-moving-data-to-the-cloud.html>> [Accessed 6 November 2020].
- [9] Bozicevic, V., 2020. How To Overcome Five Common Cloud Challenges. [online] Globaldots.com. Available at: <<https://www.globaldots.com/blog/common-cloud-challenges>> [Accessed 6 November 2020].
- [10] Blog. 2020. Top 10 Security Concerns For Cloud-Based Services. [online] Available at: <<https://www.imperva.com/blog/top-10-cloud-security-concerns/>> [Accessed 6 November 2020].
- [11] Guru99.com. 2020. Top 25 Cloud Computing Service Provider Companies (2020). [online] Available at: <<https://www.guru99.com/cloud-computing-service-provider.html>> [Accessed 7 November 2020].
- [12] Docs.microsoft.com. 2020. Quickstart: Connect With PHP - Azure Database For Postgresql - Single Server. [online] Available at: <<https://docs.microsoft.com/en-us/azure/postgresql/connect-php>> [Accessed 7 November 2020].
- [13] Docs.microsoft.com. 2020. Quickstart: Connect And Query Postgresql - Azure Data Studio. [online] Available at: <<https://docs.microsoft.com/en-us/sql/azure-data-studio/quickstart-postgres?view=sql-server-ver15>> [Accessed 7 November 2020].
- [14] Drive.google.com. 2020. Update Your Browser To Use Google Drive - Google Drive Help. [online] Available at: <https://drive.google.com/drive/folders/1quZ7cWpsVxHqgefNWyNr_QqSa6BQf-Ab> [Accessed 7 November 2020].
- [15] Toolbox. 2020. 10 Key Challenges In Cloud Computing And How To Overcome | Toolbox. [online] Available at: <<https://www.toolbox.com/tech/cloud/blogs/10-key-challenges-in-cloud-computing-and-how-to-overcome-110518/>> [Accessed 7 November 2020].