Q1
5 Points

Welcome to the CSCE 412 Final.
While there is no strict word minimum or limit, it is important that you think through your answer and build a concept. Fluff or too little information is taken as a lack of understanding and will not enhance your performance.
Take this as a time to express what you have learned and what you can do from this class.
Finally, read all the questions before starting, as they build on each other.

Q1.1 Test Environment
0 Points

All answers must meet a minimum viable solution to the questions asked to be graded.

I certify that I am in class

- ○ no
- ◉ Yes

and working with the following 3 people:

Linjian Yang

Jiayu Wu

Naixin Zong

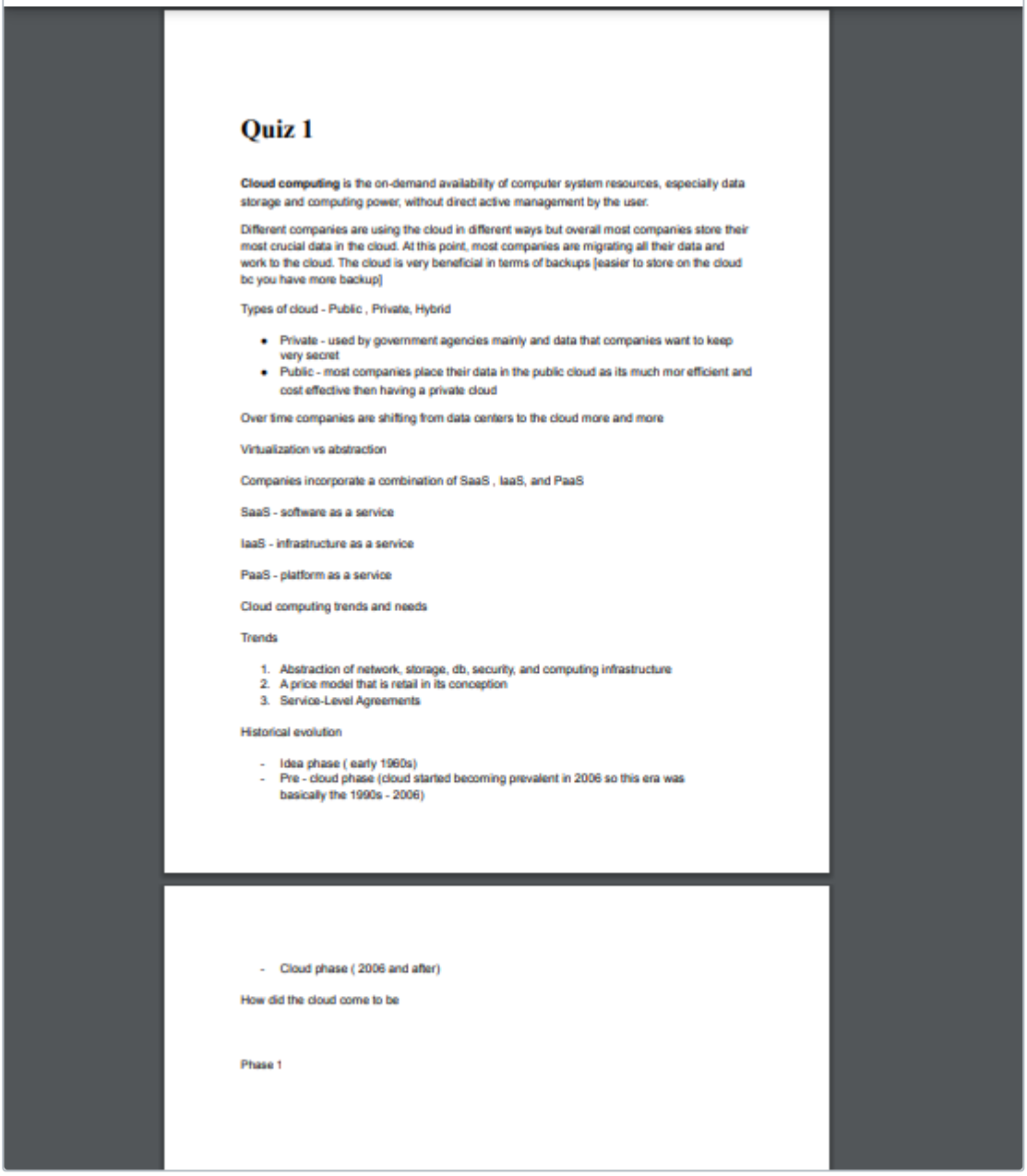
Q1.2 Notes used today

5 Points

Please upload the pdf of the notes you created and used today.

csce412-final.pdf Download

1 / 28



Quiz 1

Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user.

Different companies are using the cloud in different ways but overall most companies store their most crucial data in the cloud. At this point, most companies are migrating all their data and work to the cloud. The cloud is very beneficial in terms of backups [easier to store on the cloud bc you have more backup]

Types of cloud - Public , Private, Hybrid

- Private - used by government agencies mainly and data that companies want to keep very secret
- Public - most companies place their data in the public cloud as its much mor efficient and cost effective then having a private cloud

Over time companies are shifting from data centers to the cloud more and more

Virtualization vs abstraction

Companies incorporate a combination of SaaS , IaaS, and PaaS

SaaS - software as a service

IaaS - infrastructure as a service

PaaS - platform as a service

Cloud computing trends and needs

Trends

1. Abstraction of network, storage, db, security, and computing infrastructure
2. A price model that is retail in its conception
3. Service-Level Agreements

Historical evolution

- Idea phase (early 1960s)
- Pre - cloud phase (cloud started becoming prevalent in 2006 so this era was basically the 1990s - 2006)

- Cloud phase (2006 and after)

How did the cloud come to be

Phase 1

Q2 Current Area of Interest

25 Points

Here we will explore an area of interest.

Q2.1 Area of Interest

20 Points

Give a detailed overview (Multiple, well-written paragraphs) of the area we studied that either you are most interested in or comfortable in working/designing/engineering solutions for.

I would like to discuss the concept of data centers. Data centers' most important feature is that they provide users with shared access to data. Over time, businesses are moving away from data centers & into the cloud. There are all kinds of data centers around the world. Including data centers underwater (Microsoft) and in data centers in the coldest parts of Russia. Data centers are known to require a large landmass and require safer locations that do not have a multitude of natural disasters. Additionally, it is important to keep a data center clean (not dusty) and cool. Data centers are preferred at times as they outsource data control. Outsourcing data control decreases the odds of a power disaster/failure impacting the data.

Currently, one security issue of data centers is that you don't want your data near another company's data as whoever comes to check that data may snoop into yours so a lot of big companies have their own data centers. For this reason, companies need to distribute their data loads amongst different providers because they do not want to be locked to a specific vendor.

There is a trend that shows that data is increasingly consumed and produced at the edge. Even now data centers serve a lot of end users. There are over 7,000 datacenters serving over 25 million people around the world. Future data centers are going to be serving more and more devices found at the edge. For example: self driving cars, video surveillance (subject-object recognition), smart cities, wearables,etc. Incorporating more Artificial Intelligence into these technologies will enable better results.

Q2.2 Example

5 Points

Give a specific example of this area in use today.
Then describe its role in Cloud computing and the benefits to either the end-

user, service provider, cloud engineer, or other specific benefactor or stakeholder.

Data centers today power a multitude of platforms. For example, online gaming communities & productivity tools (notion, gmail github, etc) need data centers to function. A Data center's most important feature is that they provide users with shared access to data. Hence, if it is a situation where data needs to be accessed from different parts of the world or by different people a data center is the way to go.

Q3 Concept of a Future Development

25 Points

In this section, you will be required to make a "next logical step" from the system we have in place and have studied, to a system not yet in place. **Giant, unexplainable leaps in technology are NOT valid.**

Q3.1 Propose an Idea

20 Points

Give a detailed overview (Multiple, well-written paragraphs) of the concept you would like to develop. This must be a new development that uses current technology and expands on that.

I would like to develop solutions for cloud security. During the semester I had a lot of issues with project 1, project 2, and project 3. AWS kept telling me that I solved the captcha's incorrectly or would block certain aspects of my account in fear of not having security. Cloud Security is currently something that isn't considered or thought about heavily. I want to create a platform that easily allows secure access to their cloud computing resources (hassle-free) and blocks out bots/hackers/threats. Security issues for edge computing are denial of service attacks, data theft, data integrity/falsification, invasion of privacy, and identity authentication. unauthorized access, and activity mointoring. My solution will monitor/track threats, identify attackers, support attack recovery, and will make sure accidental/unintentional failures aren't confused with security attacks. In terms of activity mointoring hardware root of trust can be created with Secure cpu, Secure perimeter, and s ecure data

Information security can be viewed as including three functions: confidentiality, integrity, and availability. Access control determines who can access a computer system/data rightfully. Secure communications require encryption (commonly recognized as the encryption algorithm). Protection of data requires limiting the availability of data to authorized recipients & integrity checks on the data.

There are also environmental factors that affect the evolution of info security: Computing power available, Moore's law, a growing user base, and sharing of info resources. Some independents factors that I need to consider to drive the evolution of security considerations is performance and environment.There are also many Security concerns of cloud operating models. For example for Infrastructure as a Service (IaaS) users want to ensure that hardware-level services (i.e. ports and drivers) are protected from other processes running on the same physical server. Then for Software as a Service (SaaS) users want to ensure that their data is protected from other users. users data may need encryption to halt unauthorized access.Finally, for Platform as a Service (PaaS) users want to ensure that platform services can be trusted and that there is no man-in-the-middle attack. Hardware Security Models (HSM) are computing device (physical) acting as a safe to manage digital keys. HSMs provide strong authentication & crypto processing services.

When it comes to internet security. There are many key elements like Private key encryption, Secure hashing, and Public key encryption. Hashing is an info security technique to mark messages to prevent tampering.

Q3.2 Give a use case

5 Points

For the idea you proposed above, give a detailed use case, including how this changes and has benefits over the status quo.

identity authentication - DUO two factor authentication is a much better security implementation than recaptchas as AI bots are getting smarter at a faster rate than the production of recaptchas. Additionally recaptchas are not a long term solution as even now my classmates and I cannot solve some of them (they are too specific and do not have good quality pictures).

Preventive Solutions

- Multifactor authentication allows for the verification of login requests and incoming users.
Corrective Solutions

- It is possible to locate and eliminate phishing sites after identifying a pattern of attacks emanating from a specific set of IP addresses or geographic regions.

Detective Solutions

- by monitoring what happens in an account and pointing out any unusual transactions.Anti-spam detection can prevent incoming phishing emails.

Q4 Requirements for Future Development

25 Points

In this section, we explore the requirements needed for your new system and the changes to our current technology that must be developed.

Q4.1 White Paper

20 Points

Write an overview of the requirements needed (Multiple, well-written paragraphs) for the concept you would like to develop. This must show the additions or changes to the current technology.

There need to be improvements in Machine Learning, Standardization of Cloud security documentation, and more. Moving forward data centers

should not be placed next to each other. Because of scalability, Cybersecurity needs to be uptight because we no longer have local stores to store data if the public cloud is hacked millions more private information is leaked. Efforts in the cyber security sector need to be continuously increased.

There are also many Security concerns of cloud operating models. For example for Infrastructure as a Service (IaaS) users want to ensure that hardware-level services (i.e. ports and drivers) are protected from other processes running on the same physical server. Then for Software as a Service (SaaS) users want to ensure that their data is protected from other users. users data may need encryption to halt unauthorized accessFinally, for Platform as a Service (PaaS) users want to ensure that platform services can be trusted and that there is no man-in-the-middle attack. Hardware Security Models (HSM) are a computing device (physical) acting as a safe to manage digital keys. HSMs provide strong authentication & crypto processing services. Solutions for all of these need to exist.

Outsorced computing using homomorphic encryption is definitely needed. Homomorphic encryption enables computations on ciphertext data by employing a type of encryption. The Applications of fully homomorphic encryption is Client side encryption, Decentralized voting protocols,Private biometrics,Querying Encrypted Databases.

Machine Learning can be applied to security it many shapes or forms. Preventive Solutions
include Multifactor authentication which allows for the verification of login requests and incoming users. With Corrective Solutions It is possible to locate and eliminate phishing sites after identifying a pattern of attacks emanating from a specific set of IP addresses or geographic regions. Finally through Detective Solutions we can monitor what happens in an account and pointing out any unusual transactions.Anti-spam detection can prevent incoming phishing emails.

A new category of edge or fog cloud computing is being created by combining locally intelligent devices with backend cloud-based processing. This new class of cloud computing offers novel usage models, but it also raises the possibility of new vulnerabilities and widespread cyber attacks.If vendors do not adhere to interoperability standards for their edge-based devices in proprietary cloud solutions, there are additional concerns

regarding user lock-in.The rapid development of IoT-based solutions in the edge computing domain is currently held back by additional concerns regarding user data privacy and legal jurisdiction.In order to avoid any legal pitfalls, vendors and cloud service providers must discuss the policy framework with users.industry has wavered between huge focal PCs and restricted registering, bringing about half and half models adding to the winding utilization development.This currently requires

enormous focal PCs to deal with the circulated edge figuring interest.As networks become faster and machines become more intelligent enough to recognize data pattern patterns and make decisions, this trend is likely to continue.To ensure a level playing field for all players, it is essential to establish standards for the interoperability of computing devices at the edge and servers at the back end in this evolution.Hackers and security professionals are increasingly utilizing ML tools and techniques to advance their respective interests.

Q4.2 Advances in Technology

5 Points

Make a list of the advances in technology needed for your system and a justification for each.

* Interoperability between IoT devices and cloud services Edge Computing
A distributed computing paradigm known as edge computing brings data processing and storage closer to the data's sources.
will shorten response times save bandwidth.

10 edge computing use case examples
Autonomous vehicles
Remote monitoring of assets in the oil and gas industry
Smart grid
Predictive maintenance
In hospital patient monitoring
Virtualized radio network and 5G

Cloud computing content delivery

- Improvements in ML - teach machines to identify and combat attackers/attacks as hackers and security professionals are increasingly utilizing ML tools and techniques to advance their respective interests. Machine Learning in a Public Cloud.ML will help with activities, tools, techniques used to detect patterns/predict future behavior.
ML based solutions will perform specific tasks w/o external instructions

- Standardization of Cloud Security documentation: Having a standard for what cloud security looks like will require companies to secure their cloud. In turn, end users will not have to provide their own security. Information Security in the Cloud must be solved to the satisfaction of all the stakeholders in the EDA industry. This will enhance the security posture of private businesses and government agencies that handle government data. Currently lacking in standardization are Functional interfaces for SaaS (Software as a Service), Functional interfaces for PaaS (Platform as a Service), business support, Provisioning, Configuration, Security,Self-service management interfaces for SaaS,Privacy

-improvements in secure hashing
- Improved multiparty clouds (multiparty clouds are known to have better security)
- Safer implementation of Edge computing. Currently, they provide fabulous operational capability opportunities but a HUGE AMOUNT of security problems.

Cloud Computing future trends
- Quantum computing
- Edge computing
- Secure Access Service Edge (SASE)
- Cloud Regions
-Green Cloud

Q5 Projects

20 Points

We have worked on 3 projects in this class.
Answer the following questions about your projects.

Q5.1 Project 1

5 Points

Describe VMs, Virtualization, and the purpose and benefit of this.

Virtual Machine - uses software instead of a physical computer in order to deploy applications/platforms and run programs. Used by companies to test applications without purchasing multiple physical computers Virtualization - Virtualization gives an infinite number of perfectly replicated virtual machines with virtualization on demand. Virtualization aids developers in accelerating software updates, increasing software security, and maintaining an effective pipeline between development, testing, and deployment. Virtualization reduces downtime, operating cost and increases IT efficiency/productivity.

Q5.2 Project 2

5 Points

It is evident from the project 2 name, Load Balancer, what the project is intended to do. Describe other uses that could be quickly implemented by the load balancer we asked you to design and implement.

Load balancers decrease the odds of server overload and also improve the applications availability. Elastic load balancing automates process that distributes incoming app traffic across several EC2 instances.Load balancing enables automatic scaling and comes with robust security. other uses that could be quickly implemented by the load balancer is a queuing system for CSCE advising help or financial aid support.

Q5.3 Project 3

10 Points

List the services used with Namecheap.com AWS, and Git, what they did and why we used them.

Namecheap.com - registered our domain name with accreditation.

AWS S3 bucket - the data for our website (html css javascript etc) was stored in an S3 bucket. AWS S3 is an object storage system with a straightforward web service interface, and retrieved from anywhere on the internet. It is intended to be 99% durable and scale past billions of things globally. You only need to upload files to an S3 bucket and set up your S3 bucket for web hosting to use S3 for a static website.

AWS CloudFront - We used cloud front as a content delivery network. A content delivery network called Amazon CloudFront is run by Amazon Web Services. In order to improve access speed for downloading the material, content delivery networks offer a globally dispersed network of proxy servers that cache content, like web videos or other large media, more locally for customers.

AWS Route 53 - Route 53 is a scalable and highly available Domain Name System (DNS) web service. Domain registration, DNS routing, and health checking are the three main tasks that Route 53 can be used for. We utilized Route 53 in this instance for DNS routing. Route 53 assists in establishing a connection between a user's web browser and your website or web application when they open a web browser and type your domain name (example.com) or subdomain name (acme.example.com) in the address bar

AWS Certificate Manager - used to secure the website. You may provision, maintain, and renew publicly trustworthy TLS certificates for AWS-based websites with the aid of ACM, an AWS service. The operation, encryption, and security of interactions between a client and server depend heavily on certificate management.

AWS Code Deploy - Enables continues integration and deployment of the secure domain name (in my case its csce412margin.xyz) every time you update your github repository.

Github - Enables code hosting and collaboration. Multiple people can now

work on the website and deploy changes.

Final Exam

UNGRADED

STUDENT
Mualla Argin

TOTAL POINTS
- / 100 pts

QUESTION 1

(no title) 5 pts

1.1 Test Environment 0 pts

1.2 Notes used today 5 pts

QUESTION 2

Current Area of Interest 25 pts

2.1 Area of Interest 20 pts

2.2 Example 5 pts

QUESTION 3

Concept of a Future Development 25 pts

3.1 Propose an Idea 20 pts

3.2 Give a use case 5 pts

QUESTION 4

Requirements for Future Development 25 pts

4.1 White Paper 20 pts

4.2 Advances in Technology 5 pts

QUESTION 5

Projects		20 pts
5.1	Project 1	5 pts
5.2	Project 2	5 pts
5.3	Project 3	10 pts