AMERICAN INTERNATIONAL UNIVERSITY-BANGLADESH

408/1, Kuratoli, Khilkhet, Dhaka 1229, Bangladesh

Assignment Title:	Article		
Assignment No:	01	Date of Submission:	09/11/22
Course Title:	Management Information System		
Course Code:	00393	Section:	G
Semester: Fall	20 22 - 23	Course Teacher:	Danilo G. Morgia

Declaration and Statement of Authorship:

1. I/we hold a copy of this Assignment/Case-Study, which can be produced if the original is lost/damaged.
2. This Assignment/Case-Study is my/our original work and no part of it has been copied from any other student's work or from any other source except where due acknowledgement is made.
3. No part of this Assignment/Case-Study has been written for me/us by any other person except where such collaborationhas been authorized by the concerned teacher and is clearly acknowledged in the assignment.
4. I/we have not previously submitted or currently submitting this work for any other course/unit.
5. This work may be reproduced, communicated, compared and archived for the purpose of detecting plagiarism.
6. I/we give permission for a copy of my/our marked work to be retained by the Faculty for review and comparison, including review by external examiners.
7. I/we understand thatPlagiarism is the presentation of the work, idea or creation of another person as though it is your own. It is a formofcheatingandisaveryseriousacademicoffencethatmayleadtoexpulsionfromtheUniversity. Plagiarized material can be drawn from, and presented in, written, graphic and visual form, including electronic data, and oral presentations. Plagiarism occurs when the origin of them arterial used is not appropriately cited.
8. I/we also understand that enabling plagiarism is the act of assisting or allowing another person to plagiarize or to copy my/our work.

** Student(s) must complete all details except the faculty use part.*
** Please submit all assignments to your course teacher or the office of the concerned teacher.

Group Name/No.: Self

No	Name	ID	Program	Signature
1	MD. SUMON	20-42556-1	BSc in CSE	Sumon

Faculty use only

FACULTYCOMMENTS	Marks Obtained	
	Total Marks	

Data Security in Cloud Computing

Data security is safeguarding company data and avoiding data loss due to illegal access. The entails are protecting your data from assaults that can alter or damage it, as well as assaults that can encrypt or destroy it, like ransomware. Data security guarantees that data is accessible to everyone who needs it within the company.

Data security prevents digital data from being accessed by unauthorized parties, corrupted, or stolen at any point in its lifecycle. It is a notion that covers all facets of information security, including administrative and access controls, logical security of software programs, and physical security of hardware and storage devices. Organizational policies and procedures are also included. Different services are delivered via the Internet through cloud computing. These tools and programs comprise software, servers, databases, networking, and data storage, among other things. Cloud-based storage enables you to save files to a remote database rather than a proprietary hard drive or local storage device. An electronic device has access to the data and the software programs needed to run it as long as it has internet access. For various reasons, including cost savings, increased productivity, speed and efficiency, performance, and security, cloud computing is a popular choice for individuals and businesses.

Whether data is stored in public or private clouds, data security is essential in cloud computing. A few of the numerous data security issues businesses face when moving sensitive data and applications into the cloud include:

- Compliance and privacy violations
- Service provider breaches
- Exposure
- Unintentional misconfigurations of cloud services and data storage objects

Insider threats, as well as other dangers that also impact on-premises settings, have an impact on the security of cloud computing. Organizations must know the top cloud data security threats and challenges, how to mitigate them, and general and SaaS-, PaaS-, and IaaS-specific cloud requirements to benefit from the cloud.

Cloud computing services offer users several benefits, such as Email backup, storage, and information, retrieval, developing and evaluating apps, examining data, streaming audio and video, and On-demand software delivery.

Service-based and deployment-based cloud computing models are the two basic categories.

Cloud Deployment Models: Location-based deployment strategies are used in cloud computing.

To determine which deployment option would best meet the needs of the organization. Four different cloud deployment models are available. There are four types of clouds: public, private, hybrid, and community.

Public Cloud: A form of hosting in which cloud services are made available to the public across a network is known as a public cloud. Customers have no say in where the infrastructure is located. All users contribute to the cost, which is either free or takes the form of a licensing scheme like pay per user. Public clouds are fantastic for businesses that manage both the host application and the multiple user-facing applications.

Private Cloud: A private Cloud is an organization's only use of cloud infrastructure. It allows enterprises more control over security and data that is internally controlled and firewall-protected. It may be internally or externally hosted. Private clouds are excellent for businesses with strict safety, administration, and uptime requirements.

Hybrid Cloud: In private and public clouds, hybrid clouds can function independently. Resources are controlled and can be obtained from internal and external sources. For scalability, flexibility, and security, a hybrid cloud is excellent. An organization that interacts with clients using the public cloud while protecting their data in a private cloud illustrates this.

Community Cloud: It is an infrastructure that organizations that are a part of a particular community share with one another. Community members frequently share concerns about security, performance, and privacy. A community cloud at a bank, the government of a nation, or a trading company illustrates this.
Cloud service models focus on providing some offering to their clients.

Cloud Software as a Service: Software-as-a-Service, or SaaS for short, is an approach to delivering software to customers that relies on the cloud. Instead of buying and installing an application once, SaaS users subscribe to it. A SaaS application can be accessed and used online from any compatible device. The entire program executes in cloud servers that may be located far from a user's location. An app or a browser can both be used to access SaaS applications. SaaS apps are often used instances of online email services that customers use using a web browser, such as Gmail and Office 365.

Cloud Infrastructure as a Service: IaaS is a scalable subscription-based cloud computing infrastructure that offers computing, network, and storage capabilities through the Internet. Platform as a Service (PaaS) and SaaS can be built on or in addition to this basic cloud service. IaaS is a popular platform-building tool used by many agile and DevOps teams. It can scale up or down as needed because it is a subscription service, giving it more flexibility than on-premise infrastructures.

Cloud Platform as a Service: The runtime environment is provided via Platform as a Service (PaaS). It makes it simple for programmers to build, test, use, and deploy web apps. These applications are available for pay-per-use from cloud service providers and can utilize an Internet connection to access them. The cloud service provider in PaaS handles back-end scalability, so end users are relieved of the responsibility of maintaining the infrastructure.

To support the web application life cycle, PaaS consists of infrastructure (servers, storage, and networking) and Platform (middleware, development tools, database management systems, business intelligence, and more).

Cloud storage operates with ease and simplicity. Information is kept in third-party-maintained data centers that can be found anywhere in the world when using cloud storage. Because the data is on hosted servers, a web interface makes it simple to access.

Several risks and security issues accompany cloud computing and its data. However, this study will cover topics like multitenancy, public cloud storage, and virtualization related to data security in cloud computing.

Virtualization: To fully utilize the resources of the existing operating system, virtualization is a technique in which an active system image that is fully operational is captured in another operating system. Running a guest operating system as a virtual machine in a host system necessitates using a unique hypervisor component. Virtualization is a crucial component in delivering the fundamental principles of cloud computing.

Virtualization does, however, present some security risks for cloud computing data.

A hypervisor being compromised is one potential risk. If a hypervisor is weak, it may become the primary target. The entire system, including the data, may be compromised if a hypervisor is compromised. The allocation and de-allocation of resources is another risk of virtualization. The possibility of data exposure to the next VM exists if VM operation data is written to memory and is not cleared before memory is reallocated to the next VM.

Storage in Public Cloud: Another security issue with cloud computing is data storage in a public cloud. Cloud computing typically uses a centralized repository, which can be a tempting target for hackers. Storage resources are complex systems that combine hardware and software implementations. If a minor security breach occurs in the public cloud, this can expose data. It is always advised to have a private cloud if it is possible for extremely sensitive data to avoid such risks.

Multitenancy: Another significant risk to data in cloud computing is shared access or multitenancy. It is dangerous for more than just one user because multiple users utilize the same shared computing resources like CPU, storage, memory, etc.

But for several users in such circumstances, sensitive information is always likely to reach other users unintentionally. Because a single flaw in the system could give a different user or hacker access to all other data, multitenancy exploits can be complex. These problems can be avoided by judiciously authenticating users before granting them access to the data. Several authentication techniques are used to prevent issues with multitenancy in cloud computing.

Cloud service providers and computing have to face many challenges, particularly security issues. The significant difficulties involved are:

Lack of appropriate governance: The service provider is in complete charge of cloud computing. The risk of losing control over authority parameters when this control is given to the provider exists. Cause security to be compromised, which causes issues with data access and resource application. When service level agreements with the service provider are absent, the threat of a security coverage gap is also present due to the compromised security issue. Furthermore, the terms of use are flexible, making it simple to take advantage of users' access to data. The Google search engine, for instance, states that the user agrees that For any content and other communications are maintained or transmitted through the service. Google disclaims all liability and responsibility and disclaims all liability and responsibility for any unauthorized access, data loss or deletion, corruption, or other types of access, including damage to the application. Customers must therefore worry about the security of their data and applications when they are hosted by a third party, service provider, or intermediary.

Isolation failure: Due to cloud computing's multi-tenancy, resource sharing is already a dubious characteristic. For businesses, a lack of separate storage can be fatal. Other issues with guest hopping attacks and their problems include a significant barrier to using and implementing cloud computing applications. The architecture of cloud computing can occasionally put customers' security and privacy at risk. Despite its rarity, this risk is very challenging to manage. Administrators and managers of cloud service providers are two examples of people who occasionally act maliciously and endanger the security of users of cloud computing applications.

Insecure or incomplete data deletion: When a client requests that data be deleted entirely or partially, it is unclear whether the requested portion of the client's data segment can be accurately deleted. This makes it more difficult for customers to sign up for cloud computing services.

Compromise of management interface: Since resources are accessible to the service provider and cloud computing services are delivered remotely over the Internet, third-party access may lead to malicious activities. As a result, there is an increase in vulnerabilities, service provider involvement, and service manipulation. By creating no-go zones in cloud computing applications, the customer could take control of the machines, and vice versa, the provider, could take control.
Other security-related issues include information transfer between cloud computing applications, data leakage while being uploaded to the cloud, attacks on the security and privacy of user data, loss or malicious manipulation of encryption keys, and disagreements between service providers and clients over protocol and policies. The integrity of cloud computing applications is not directly impacted by challenges that directly interact with or influence cloud computing. Examples of these scenarios include changes to network traffic, network outages, and administrative problems like inefficient resource use, traffic jams, and disconnected users. Other dangers connected to cloud computing applications include the possibility of social engineering attacks, natural disasters, and equipment theft.

Different encryption methods can be used for transit data and at rest. For instance, while encryption keys for data at rest can be kept for extended periods, they may be short-lived for data in transit. Various cryptographic methods are employed to encrypt data.

The current data. Thanks to cryptography, the level of data protection for ensuring content integrity, authentication, and availability has increased. Using an encryption key, the plaintext is converted into cipher text in the most basic form of cryptography. The cipher text is then decrypted using a decryption key, as shown in the diagram.
Usually, there are four primary uses of cryptography:

Block Ciphers: A block cipher is a data encryption algorithm that applies a cryptographic key and algorithm to a data block rather than one bit at a time to produce cipher text. By using this method, it is ensured that messages containing similar blocks of text are encrypted differently. Typically, the next encrypted block in a series uses the cipher text from the previous encrypted block.

Stream Ciphers: Since it depends on the current state of the cipher, this data encryption method is also known as a state cipher. Instead of using data blocks, each bit is encrypted in this method. Each bit is subjected to an algorithm and an encryption key one at a time.

Due to their low hardware complexity, stream ciphers perform faster than block ciphers.

If this method isn't used correctly, it could lead to serious security issues. Instead of encrypting blocks of text, stream cipher uses an encryption key for each bit. The resulting cipher text is a stream of encrypted bits that can be recovered to its original plain text using a decryption key.

Hash Functions: In this method, an input text is transformed into an alphanumeric string using a mathematical operation known as a hash function. The length of the generated alphanumeric string is typically fixed. This method ensures that no two lines can produce the exact alphanumeric string. The output string created through them may differ significantly even if the input strings are slightly different.

This hash function can be effortless, like the one in equation (1), or very complex.

$F(x) = x \bmod 10$ (1)

All of the techniques mentioned above and methods are frequently used to encrypt data in the cloud to guarantee data security. The application of these strategies varies depending on the situation. It is strongly advised to ensure data safety in private and public clouds, regardless of the method used. The trend of improving cloud data storage methods is undoubtedly growing with the increased use of cloud computing for data storage. Data stored in the cloud may be in danger if not adequately protected.

Even though cloud-stored data are already encrypted, security can still be increased. Data can be encrypted before being uploaded to the cloud and decrypted once retrieved. However, this can be a hassle and restricts what can be done with the data while it's being stored. It is possible to tell whether a file has changed since uploaded using the same encryption software used to protect data. People can tell if their data has been altered in this manner. Using a complex password to protect sensitive information is still a good idea.

Two-factor authentication offers an additional layer of security, which involves connecting to a cloud-based service using a password and a randomly generated, time-sensitive "token." Data kept in the cloud is frequently encrypted to thwart thieves, hackers, and nefarious governments. However, criminals also employ encryption to cover up unlawful activity. In the past, court orders and subpoenas have been used by law enforcement and intelligence agencies to obtain data from service providers like phone and Internet companies. The provider, however, cannot provide the key to the government agencies because it does not possess encrypted data. As a result, law enforcement and intelligence organizations have requested strategies to ensure they always have access to the data they require. If governments choose to provide access to encrypted data, they have several options. They could demand information from a cloud computing company that was permitted by law. They might mandate that manufacturers of devices or service providers always keep a way to access data.

However, these options come with trade-offs. While providing access capabilities helps law enforcement, adding them weakens security. U.S. companies risk losing market share if comparable restrictions are not enforced in other nations. Additionally, if only one encryption method is permitted, innovation in encryption technologies may be slowed.