Advanced Cloud Computing

**Submitted by**

ADRI SAHA

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (CSE)

1. **How does the implementation of MFA enhance the security of a Cloud-based banking system?**

**Ans:** Two-factor authentication means that each app or service you login to double-checks that the request came from you by confirming the login with you in a separate location.

You've probably used MFA before, even if you didn't know it. For example, if a website has ever sent a numeric code to your phone that you must enter to gain access, you have completed a multi-factor transaction.

MFA is essential to web security because it immediately neutralizes the risks associated with compromised passwords. If the password is hacked, guessed, or even fraudulent, this is no longer enough to grant access to the intruder: without the backing of the two factors, the password alone is useless.

MFA also does something necessary to maintain a strong security posture: it actively engages users in the security process and forms a condition in which users are informed. stakeholders about their digital security. When the 2FA notification comes to users, they must answer: "Did I do this or is someone trying to access my account?" » This emphasizes the matter of security in all transactions.

1. **What types of green IT initiatives are commonly utilized in cloud-based banking systems to reduce environmental impact?**

**Ans:** Financial institutions can use cloud computing to shift their business to a virtual environment, which may reduce energy consumption and leave a less carbon footprint on the environment.

**Energy Consumption:** Implementing virtualization, can reduce physical hardware use which may reduce energy consumption.

**Paperless activities:** By engaging in digital transformation like digital transactions and digital documentents management, paper usage and waste can be reduced.

**Digitized system:** By making IT operations digitized, remote work and using online tools reduce the need for commuting and office space and thus it lowers carbon emissions.

**Sustainable Data-Centers:** Reduce the environmental impact by using renewable energy sources, cooling systems, and energy-efficient hardware.

**Carbon Footprint:** Cloud-based services provide cloud computing resources which need on-premises infrastructure. So it saves energy and reduces Carbon footprint.

1. **How does cloud computing contribute to business continuity and flexibility?**

**Ans:** **Business Continuity:**

The cloud service provider is reliable for handling different technologies. Financial institutions may require higher levels of data security, fault tolerance, and disaster recovery. Cloud computing can handle high levels of data redundancy and backup recovery at a lower cost.

**Business Flexibility:**

With cloud computing, less infrastructure investment is required and initial setup time is reduced. In addition, it enables a faster and more efficient response according to the needs of bank customers. The cloud helps companies solve various services such as maintenance, software patches, and other IT problems. Therefore, financial institutions can focus on business and not IT.

1. **What measures can online banking systems implement to ensure the effectiveness of both scalability and security?**

**Ans:** Online banking systems can implement multi-factor authentication (MFA) to ensure the effectiveness of both scalability and security.

**MFA(Multi-factor authentication):** By implementing MFA, a user goes through multiple types of verification systems such as passwords, OTP/tokens, biometrics. So, it can ensure security without sacrificing scalability.

**Automated monitoring and Regulatory Compliance:** Regular checking and ongoing system activity monitoring can help in quickly identifying security flaws or scalability problems by enabling early mitigation.

**Encryption techniques:** During transmission and storage in banking, encryption of sensitive data keeps them safe from unauthorized access. So, it can help online banking systems in maintaining security while handling more users.

**Data location and Segregation:** Following contractual obligations, cloud computing ensures that data is safely stored and processed in a scalable environment. Segregating different sets of data also prevents unauthorized access.

**Data recovery:** If customers are unaware of their location of stored data, cloud providers can clarify disaster recovery services. Storing data by multiple sites should be enhanced safely.

1. **How do banking institutions ensure efficient data recovery and disaster response within cloud environments and what challenges arise in the process of recovering data across multiple locations?**

**Ans:** Banking institutions ensure efficient data recovery and disaster response by cloud environment using following measures:

1. **Redundant Data Storage:** To reduce risk of data loss, implementing redundant storage across several locations is useful.
2. **Automated Backup:** Using an automated backup system ensures data availability in the event of primary system failure as it regularly copies data into secondary sites.
3. **Plans for disaster recovery:** In the emergency case, comprehensive plans for data recovery should be developed including both system recovery and restoration.
4. **Testing and validation:** Test and validate the recovery plans on a regular basis.
5. **Collaboration with cloud service Providers:** Support cloud service providers by using their infrastructure for data redundancy and recovery.
6. **Data encryption and safety:** By using strong encryption and security mechanisms, protect data during the storage, transmission and recovery phases.
7. **Constant Monitoring:** Keep monitoring for any unusual activity or threats that can affect the availability or integrity of data in cloud environments.

**Challenges:**

1. **Data Consistency:** It might be challenging to ensure data consistency if data is across multiple locations. Especially, if modification or updates occur during data recovery, it will be challenging and might disrupt the system.
2. **Compliance and legal issues:** Complying with legal and regulatory obligations in many places related to data privacy can be difficult.
3. **Network disruption:** This can slow down the speed and effectiveness of the recovery process from remote areas.
4. **Data Fragmentation:** Distribution of data across multiple locations can vary difficulties in locating and retrieving every necessary component during the recovery process.
5. **Resource Allocation:** It can be difficult to allocate enough resources like bandwidth and storage capacity to enable data recovery across different locations.
6. **Cooperation and communication:** It is necessary to effectively coordinate and communicate with teams and charge who are responsible for a seamless and efficient recovery process.
7. **Security Concerns:** While accessing data from external locations or third-party providers, ensure the security of data during the recovery process is difficult.
8. **What role does transaction monitoring play in detecting and preventing fraud in online banking and what are the main challenges to implement effective monitoring mechanisms?**

**Ans:** Transaction monitoring help in detecting and preventing fraud in online banking through:

1. **Pattern recognition:** The system can identify possible fraud by looking for unusual patterns or behaviors that differ from the user's usual activity by examining transaction history.
2. **Real-time detection:** Quickly identify and address questionable activity and reduce possible losses.
3. **Fraud Pattern Analysis:** By using historical data and previous fraud patterns, the system is able to identify well-known fraud schemes and stop similar fraudulent transactions from occurring.

**Challenges:**

1. **False Positives:** It has the potential to generate false positives like marking real transactions as suspicious which often inconvenience and inefficient for users.
2. **Adaptability:** Since fraudsters are always changing their strategies, transaction monitoring systems find it difficult to identify new types of fraud.
3. **Data Quantity:** Processing and analyzing massive amounts of transaction data in real-time can be difficult. A strong infrastructure and sophisticated analytics tools are needed to overcome these problems.
4. **What are the limitations of current support services in cloud computing and how can automated monitoring and tracking mechanisms enhance security and compliance?**

**Ans:** The main limitation of current support services in cloud computing is constantly shifting data centers and the complexity of shared.

By providing real-time information and preventative measures in response to emerging threats automated monitoring and tracking systems can improve security and compliance. Organizations are able to identify errors, unusual movements, or possible dangers in real time by examining these real-time data streams. To address potential vulnerabilities or non-compliance issues, these methods can enhance security and compliance.

1. **What are the effects of security models for online banking systems on customer trust and how can banks ensure transparency in their communication regarding security measures?**

**Ans:** The security models for online banking systems play a significant role in developing customer’s trust. They feel comfortable making purchases online when they believe that their financial information is safe.

To ensure transparency in their communication regarding security measures banks can adopt some measures:

**Clear and accessible information:** Banks may provide their (Bank detail) information via customer channels, mobile apps or their websites. So they can build customer’s trust.

**Regular updates:** Banks must notify customers on a regular basis of any updates or modifications made to security protocol. This could be alerts about possible security threats, modifications to authentication procedures, or updates on new security features.

**Transparency:** Transparency in incident response: Banks need to communicate openly with their clients in the case of a security issue or data theft. Customers who are impacted should be immediately informed.

**Educational resources:** Banks can offer customers educational resources to help them understand the value of security measures and how they can help maintain the security of their accounts. This could contain suggestions on how to identify scams, make secure passwords, and make efficient use of security features.

**Collaboration:** Banks should work with industry partners and authorities to stay updated on new cyber security threats and best practices. By participating actively in industry forums and sharing information with customers, banks can show their security commitment and transparency.

Overall, customers' trust in online banking systems must be built and maintained by communicating security measures in a transparent manner.

1. **How do cyber risks such as phishing and DDoS attacks affect cloud banking security and how can banks mitigate them?**

**Ans:** Cyber risks including DDoS, phishing, and man-in-the-browser plays a major threat to cloud banking security.

**Phishing:** It attempts to trick users to expose personal information.

**DDoS:** Distributed Denial-of-Service (DDoS) attack is a major cyber crime which happens when a hacker floods a server with excessive traffic. So that it becomes difficult for users to access the online services and linked websites.

**Man-in-the-browser:** This technique intercept and modify user communication with financial systems to collect personal information of users.

To protect against these threats, bank can implement:

* Multi-factor Authentication (MFA)
* Real-time monitoring
* Data Encryption
* Secure communication protocols
* Leverage cloud based security solutions
* Regular security audits and employee training program

1. **What are the results of using secure VPN connectivity to protect browsers from malware in online banking systems and how it improves the banking security?**

**Ans:** Using secure VPN(Virtual Private Network) connectivity in an online banking system improves security by preventing unauthorized access, enhancing browser protection, preventing malware threats, strengthening authentication techniques and safeguarding against cyber attacks.

**Improves banking security:**

1. **Enhanced Authentication:** Browsers with VPN support provide safe connections to the banking system by adding an extra layer on top of the standard login information. This helps in user identification verification and protects against illegal access.
2. **Enhanced browser protection:** Secure VPN connectivity protects the browser from attacks and malware access. It provides a safe, encrypted tunnel between the user’s device and online banking system.
3. **Prevention of unauthorized access:** By using VPN connectivity, risk of unauthorized access attempts is minimized.
4. **Protection against keyloggers:** VPN environments significantly reduce the danger of keyloggers attacks by encrypting keys and preventing malicious programs from accessing important information including login passwords or financial data.
5. **Explain the working principle of Multi-Factor Authentication Architecture in the banking Sector?**

**ANS:**

Multi-factor authentication (MFA) in banking works by requiring users to provide two or more forms of identification to access their accounts or securely complete transactions. It involves the following steps:

1. **Identification**: Users initiate login or transaction processes by providing a username or account number.

2. **First Factor Authentication**: After entering their identification, users provide the first authentication factor, typically a password or PIN.

3. **Second Factor Authentication**: Following successful validation of the first factor, users must provide a second form of authentication. This could be something they own (e.g. a mobile device to receive an OTP), something they own (e.g. biometrics like fingerprints or facial recognition), or something related to the location of their mind.

4. **Transaction verification:** For high-risk transactions, users may receive a notification prompting them to confirm or decline the transaction.

5. **Backend Authentication**: The banking system verifies each authentication factor against its records or authentication server. Access is granted only when all provided factors match stored information and security policies.

MFA improves security by adding layers of authentication, making it more difficult for unauthorized users to access accounts or engage in fraudulent activity. It protects sensitive financial information and minimizes risks associated with unauthorized access and use.

1. **Expose the problems that arise in the security of the banking system.**

**Ans:** There are several challenges that arise in ensuring the security system in banking organizations.

1. **Cyber threats:** Banking systems have several cyber threats like malware, phishing attacks, DDoS attacks, and man-in-web-browser attacks. These cyber-attacks can constantly hack sensitive data from users and disrupt service.
2. **Regulatory compliance:** Severe regulations like those related to data security, privacy, AML (anti-money laundering), and KYC (know-your-customer) should be followed by banks. This makes security management more difficult.
3. **Third-party risks:** Banks often integrate with several third-party services like payment processing and data storage. If these third-party apps or services have inadequate security measures it can add additional risk to banking security.

In short, we can say A complete approach to cybersecurity is needed to address these issues. One that involves training employees, frequent risk evaluations, the use of advanced security technology, and cooperation with industry partners and regulators.

1. **Note the importance of cloud computing in the online banking system?**

The importance of cloud computing in the online banking system can be summarized as follows:

**1. Scalability:** Allows banks to easily scale their resources based on needs without much initial investment.

**2. Flexibility:** Enables rapid deployment of new features and updates to adapt to changing market needs.

**3. Cost-effective:** Reduces capital and operating costs associated with maintaining physical infrastructure.

**4. Reliability:** Provides high availability, redundancy, and disaster recovery to ensure uninterrupted banking services.

**5. Security and Compliance:** Provides robust security features and a compliance framework to protect sensitive data and meet regulatory requirements.

6. Innovation: Facilitate the integration of new technologies and services to improve user experience and drive customer engagement.

Overall, cloud computing enables online banking systems to provide secure, reliable, and innovative services while optimizing costs and ensuring compliance.

1. **How does the elasticity of usage-based billing in cloud computing affect cost savings and resource distribution for banks and financial institutions?**

**Ans:**

The elasticity of usage-based billing in cloud computing provides banks and financial institutions with several benefits that contribute to cost savings and efficient resource distribution:

**1. Cost-effective:** Usage-based billing allows banks to pay only for the IT resources and services they use, allowing them to optimize costs and avoid over-provisioning. Banks have the flexibility to increase or decrease resources based on need, reducing waste and minimizing unnecessary spending.

**2. Resource Optimization:** Banks can leverage flexibility to allocate resources more effectively, ensuring there is enough computing power, storage, and network bandwidth to support operations and your application. This flexibility allows the bank to adapt to fluctuating workloads and seasonal changes without sacrificing performance or user experience.

**3. Scalability:** Elasticity allows banks to quickly scale infrastructure resources to meet growing business needs, spikes in user traffic or product launch a new product. Banks can easily add or remove resources as needed, ensuring they can scale their operations according to business growth and customer needs without the need for additional investment. hardware or infrastructure.

**4. Improved performance:** By dynamically adjusting resource allocation based on workload requirements, banks can ensure optimal performance and responsiveness for online banking applications, their transaction processing systems, and customer-facing services. Elasticity allows banks to maintain consistent service levels and meet performance SLAs, even during peak usage periods or traffic spikes.

**5. Flexibility and innovation:** Usage-based billing and flexibility enable banks to test new technologies, services and applications without incurring large upfront costs or commitments. long-term conclusion. Banks can rapidly provision and test new environments, deploy innovative solutions, and iterate on their services to drive digital transformation, improve customer experience, and achieve gain a competitive advantage in the financial services industry.

Overall, the elasticity of usage-based billing in cloud computing enables banks and

financial institutions to optimize costs, improve resource utilization, scale

their operations efficiently, enhance performance, and drive innovation. By

leveraging elasticity, banks can adapt to changing market conditions, customer

preferences, and regulatory requirements while maintaining agility and cost-effectiveness in their IT infrastructure and operations.

1. **How does regulatory compliance impact cloud platforms in financial institutions?**

**Ans:** In financial institutions, though user’s information is stored by the bank provider, the responsibility for data security and integrity lie with users. So, regulatory compliance has a significant role in cloud platforms in banking systems.

1. **Data Security:** Regulatory requirements often follow some measures that financial institutions need to implement to ensure data security, access control, encryption, and confidentiality of users.
2. **Risk management:** Regulatory compliance also addresses some risk management practices like identifying vulnerabilities, controlling implementations, and developing event responses. These are required to mitigate potential risks involved with cloud performance.
3. **Legal Obligations:** Banks are supposed to bind with various laws and regulations including data protection, privacy and security. So, it is mandatory to comply with these regulations. Otherwise, failure will result in several penalties like demotion of growth, fines and legal steps.
4. **Audits and Reporting:** Regulatory compliance involves regular audits and reporting trust by the applicable laws and regulations. Cloud platforms must support these requirements by allowing monitoring, logging and reporting capabilities.
5. **Data Sovereignty:** Sensitive data can be stored and processed where regulations meet some restrictions. Financial institutions that use cloud platforms that span many geographical locations must ensure data sovereignty.

In short, we can say regulatory compliance affects several aspects and so it has become a crucial factor for financial institutions using cloud platforms. Compliance ensures the security of customer data and maintains the trust and reliability of financial institutions among customers and regulators.

1. **How can the security vulnerabilities of OTP tokens be addressed effectively?**

**Ans:** OTP tokens can be addressed effectively in various ways. Financial institutes can implement MFA (Multi-Factor Authentication) using OTP. Time-based OTP is used to limit the validity period of passwords. Also, it ensures strong encryption for communication, securely manages the token lifecycle, and stores tokens on trusted platforms. OTP implies security concerns for customers and frequently monitors suspicious activities. So, these measures collectively improve the security of OTP which adds an extra layer to MFA and so OTP mitigates the risk of unauthorized access or misuse.

1. **How does CAPTCHA help prevent automated attacks on banking systems?**

**Ans:** One of the main uses of CAPTCHA (a fully automated public Turing test to distinguish computers from humans) is to prevent online automated password attacks. This is why many financial institutions have implemented CAPTCHA on the login page of their e-banking systems to protect customers against such attacks.

1. **Two Approaches to Breaking Captcha:** To launch a MitM attack on Captcha, the attacker (i.e., the malicious program) needs to manipulate the transaction data in real time without being noticed by the user.
2. **Automated Attack 1:** In this attack, the malicious program achieves transaction manipulation via the following steps

* **Step 1: Locating transaction data:** Step 1 is to further locate transaction data from the text layer segmented from the Captcha image.
* **Step 2: Removing transaction data:** After locating the line with transaction data, we can try to remove the whole line by applying an image inpainting method.
* **Step 3: Adding user-expected transaction data:** After removing the transaction data, it is trivial to add the user-expected transaction data to the vacant place in the Captcha image.

1. **Automated Attack 2:** The image-inpainting-based attack described above is blind, in the sense that it does not depend on a recognition task. However, if we can recognize the user’s birthday and the TAN index embedded in the Captcha image, a second attack can be developed.

* **Stage 1: Offline birthday recognition:** As shown in Sec, the image segmentation process can produce a segmented layer with a birthday.
* **Stage 2: Online transaction manipulation:** Once the user’s birthday is broken, the malicious program can start manipulating transaction data and forging Captcha images.

1. **Human-involved semi-automated attack:** In Automated Attack 2, the first stage is to recognize the user’s birthday, which is done offline.
2. **Efficiency of the proposed attacks:** For 100 test images, the average running time of the inpainting-based attack is around 250 ms and that of Stage 2 (online transaction manipulation) of the recognition-based attack is around 190 ms.
3. **What are the key challenges for online banking systems security due to increasing transaction volumes and the threat of malware and cyber-attacks?**

**Ans:**

**Cyber Threats:** There are a lot of challenges banks have to face during the changing environment of cyber threats like malware attack including spy-eye, phishing, DDoS, cross-site and man-in-the-browser attacks. To mitigate these risks constant attention to detail and preventive measures are needed.

**Credential Validation:** Hackers frequently use techniques like phishing and pharming to attack login credentials. As transaction volumes rise, it becomes more difficult to ensure that user credentials are validated particularly for remote connections.

**Cloud protection:** Nowadays, as cloud-based technologies become more widely used, it has become difficult to ensure security of online banking systems. Financial institutes need to handle cloud based security issues such as access control, compliance and data safety.

**Multi-Factor Authentication (MFA):** While handling numerous transactions, having a strong MFA system in order to improve security adds more complexity. It is essential to find a balance between user comfort and security measures.

**Regulatory Compliance:** Keeping regulatory requirements regarding privacy and data security adds additional complexity. Banks must maintain efficient security measures with regulations while maintaining requirements.

**Scalability:** Online banking systems must scale effectively to accommodate rising transaction volumes without losing security. Strong infrastructure and flexible security measures are necessary for this.

1. **Write down the components of Multi-Factor Authentication (MFA)?**

**Ans:** MFA (Multi-Factor Authentication) functions by instructing more verification information (factors). One of the most common MFA factors that users encounter is one-time passwords (OTP). OTPs are those 4-8 digit codes that you often receive via email, SMS, or some sort of mobile app. With OTPs a new code is generated periodically or each time an authentication request is submitted. The code is generated based upon a seed value that is assigned to the user when they first register and some other factor which could simply be a counter that is incremented or a time value.

The components of Multi-Factor Authentication (MFA):

* **Knowledge Factor:** Password, PIN, Security Question, Captcha
* **Possession Factor:** Token/OTP/Smart Card
* **Inherence Factor:** Fingerprints, Facial Recognition, Psychological Characters

1. **Write down the key components and features of cloud-based architecture?**

**Ans:** In cloud computing, frontend platforms contain the client infrastructure—user interfaces, client-side applications, and the client device or network that enables users to interact with and access cloud computing services.

The key components of the cloud-based architecture:

* A frontend platform
* A backend platform
* A cloud-based delivery model
* Network (internet, intranet or intercloud)

Cloud computing has many features that make it one of the fastest-growing industries today. The flexibility offered by cloud services in the form of their ever-evolving suite of tools and technologies has accelerated their deployment across industries. This blog will tell you about the essential features of cloud computing.

The features of cloud-based architecture:

* Resources Pooling
* On-demand self-service
* Easy Maintenance
* Scalability And Rapid Elasticity
* Economical
* Measured And Reporting Service
* Security
* Automation
* Resilience
* Large Network Access