FINTECH

CIS 8087 Cloud Computing and Security —

Fintech: Choosing a Cloud Services Provider

Fall 2022

By: Montez Bell, Wonik Kim, and Venkat Sai Nag Bhargav Sabbineni

Contents

Executive Summary

The case focuses on Fintech, a corporation that provides payment and billing services to the alcoholic beverage industry. Joe Kwo, the company's chief information officer, was tasked with selecting a cloud service provider for the new service that gives analytical data to the company's customers. The CIO informed his colleague about the plan to develop a cloud-based solution. Kwo and his team were tasked with deciding between Google Cloud Platform, Amazon Web Services, and Microsoft Azure. The three firms met the criteria for Fintech, yet they had significant disparities. In this instance, the corporation investigates the host's choices to get the cloud service. Once the host company was chosen, the CIO had to determine how to launch, operate, and manage the new services while maintaining customer relationships and mitigating the inherent risks of cloud computing.

Introduction

The firm had a responsible IT department but selecting a solid cloud service provider was vital. Joe Kwo and his coworkers are tasked with establishing a system for analyzing data for cloud computing. To prepare a report based on data analysis, the IT staff utilized customer data and required the data in two formats: data access tool or CVS file format, which allowed them to format the data in Microsoft Excel.

Before deciding which cloud service to implement, Fintech needed a thorough understanding of the numerous cloud service kinds and their distinctions. Two forms of cloud computing were accessible, namely Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) (IaaS). According to PaaS, the service provider would manage and control the infrastructure and its applications. Infrastructure as a Service provider would own and operate the servers, while the company's IT department would install and manage its middleware and development tools. Cloud computing allowed businesses to rent cloud services rather than make costly software and computer expenditures. Recognizing the benefits of cloud computing, the CIO was aware that adopting cloud computing would present challenges, particularly security concerns.

Fintech was seeking scalability on the cloud. In past years, EFTPS successfully processed many payment transactions, and its client base expanded quickly. Consequently, a cloud-based solution was required. Amazon, Microsoft, and Google, the three cloud service heavyweights, provided exceptional cloud support and services. In such a case, Fintech was needed to examine each company in detail, considering economic factors such as (total cost of ownership, initial price, and complementary investments), human factors such as (presence and skills of local consultant and provider, analytic and IT staff), and security and technical factors such as (scalability, programmability, support, and database), among others. After weighing several factors, the CIO selected Amazon as their cloud service provider due to Amazon's reduced support costs compared to Microsoft and Google. They all looked to offer comparable services, but Amazon's services were less expensive.

Joe Kwo's coworkers believe in his decisions to ensure Fintech's success. The executive team thought that the new system would enhance the company's connection with its customers if it performed flawlessly. The CIO was acutely aware that if the system failed to fulfill the customer's expectations for system dependability and data quality, consumer satisfaction would rapidly decline. The company's IT department performed a remarkable job of explaining the critical distinctions between each cloud-based service provider. Amazon, Google, and Microsoft satisfied every condition on Kwo's list, but the discrepancies were significant.

Root Problem

Fintech must overcome various technical obstacles to provide the new cloud service. The ongoing evolution of IT is one of the most challenging technological concerns we confront. New technologies will always be less efficient than their older counterparts in the long term. Nonetheless, the cloud service will continue to gain additional features as they become available. In addition to other technological difficulties, Fintech will have to contend with data theft and breaches. Financial technology companies are in danger of data theft. Two methods exist for compromising a cloud account: theft and hijacking. In the future, it may be necessary for the financial technology industry to create solutions for handling data breaches. Data theft may be the cause of cloud service information loss. Fintech will also be susceptible to denial-of-service (DoS) assaults. If you initiate a DOS assault, you flood the system with data to overwhelm it. Security difficulties arise for technical reasons. The disadvantage of cloud computing is that it is impossible to determine precisely where your data is being handled.

Consequently, the development phase of the project carries a greater chance of encountering issues. Not a single data breach or interface hacking instance has been recorded. One of the business issues that Fintech may encounter is maintaining positive relationships with clients after implementing the cloud service. Several considerations must be made to retain a client. Among them is customer satisfaction, preserving consumer expectations, and possessing a reliable, effective system that not only meets but surpasses customer expectations.

It is also possible that the company will incur significant management costs, which will be a challenge because developing a cloud service with precisely defined and addressed needs is a technical obstacle that must be surmounted if the company wishes to deliver the quantities its customers expect from cloud services. Failure to do so might result in financial losses for the firm, even if there is no physical damage. This section primarily concerns three cloud service providers: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). There are several similarities and distinctions between these three enterprises. Pay-as-you-go is available from all three cloud service providers, although the monthly rates vary significantly.

Key Questions

1. Joe Kwo recognizes that the cloud offers both opportunities and risks.
    a. How would a move to the cloud make it easier and/or more profitable for Fintech to provide large volumes of selected data to its clients?

This question primarily concerns IT's constant evolution and double-edged sword nature. In his role as CIO, Joe Kwo will need to evaluate cloud computing from the perspectives of a general manager and an IT manager in an organization undergoing business and technological transformations. Similar may be the case concerning other Fintech rivals, which may be doing this, influencing a subset of consumers who wish to access their data via the cloud. Moving their data to the cloud will be advantageous for Fintech in several ways.

Less financial risk will be among the benefits. Although beginning expenses will be significant, assessing security needs, conducting testing, and establishing the cloud service will be entirely advantageous. Fintech will cut their expenditures in hardware and software necessary if cloud bases are not implemented (Huth & Cebula, 2011). When providing this service, it would be simple for the corporation to reach break-even and generate profits.

If Fintech does not have considerable expertise with cloud computing, a rival will capture not just existing but also targeted consumers with similar cloud-computing services. Therefore, this will be pretty advantageous for the company. However, the company may rent the service to other cloud-based providers. Otherwise, this will yield greater profits for the institution.

b. What technical challenges does Fintech face in offering the new service?

Fintech has a variety of technical obstacles while introducing the new cloud service. IT evolution is one of the technological difficulties. Emerging technologies will always be inferior to their competitors. However, new features will constantly be added to the cloud service. In addition, data theft and data breaches are some of the technological obstacles that Fintech will confront. Fintech may be susceptible to data theft. This refers to a cloud account that has been either stolen or compromised. Fintech may be required to provide solutions for data breach situations. Data theft might result in the disclosure of sensitive information via cloud services. DoS attacks are an additional technological obstacle that Fintech will encounter. A DoS attack will result in the system being flooded with data to overload the system. Technical considerations lead to security problems. A characteristic of cloud computing is that the location of data processing is uncertain. This raises the potential hazards associated with the project's implementation. Cases of data breaches and interface hacking have not been addressed, and this is, in fact, the most significant technological problem of cloud services.

c. What business challenges does Fintech face in offering the new service?

After introducing a cloud service, one of the business issues that Fintech may encounter is maintaining positive client connections. To retain customers, it is necessary to examine several things. They include customer happiness, meeting and exceeding customer expectations, and having a dependable system that meets and exceeds consumer expectations. In addition, the administration cost may be high, posing difficulty for the business, as it may be challenging to build a cloud service with the exact specified and forecasted volumes that customers want. This will occasionally result in corporate losses or lower-than-anticipated earnings.

2. Assume Joe Kwo will choose a cloud services provider today. Based only on information provided in the case, which provider should he choose? Why? You will need to compare the three cloud services providers' offerings in detail and be ready to discuss the technical and business implications of those differences.

This section will evaluate AWS, Microsoft, and Google as cloud service providers. There are parallels and contrasts between these three firms. Although all three cloud service providers provide a pay-as-you-go pricing model, their monthly fees differ. AWS is the least-priced option, whereas Microsoft is the most expensive. High pricing might deter prospective customers who will choose the less expensive option. In addition, AWS accepts local money, unlike other cloud service providers. This is significant for users outside the United States, as they will pay in their own countries for AWS services. In addition to providing their services through mobile devices and other channels, the three service providers make cloud services accessible anywhere. In addition to providing a mobile app for Android and iOS, AWS offers customer help where potential customers may receive answers to various inquiries and instructions. Microsoft provides a mobile application that is compatible with both Android and iOS. In a time when anybody might request data and cloud services, the emergence of mobile applications for cloud services has played a crucial role. Mobile applications have made it simple for cloud service customers to access their data anytime and without constraints.

The databases utilized by the three cloud service providers relate to one another. AWS has used databases that are like those of Microsoft and Google. In addition to employing SQL and the cloud as their server, cloud service companies have also employed Oracle and RDS for data management. This is significant since it helps organizations track their data and provides a variety of storage platforms for customer information. However, AWS has a greater storage capacity than Microsoft and Google, making it a suitable cloud solution for businesses with massive files.

A cloud services provider's primary objective is to promote the vast array of services that are accessible at a reasonable price. Although both Microsoft and Google provide dependable and comprehensive benefits, I suggest Amazon AWS to Joe Kwo. AWS provides reservable services that reduce the cost of computer pricing for one- to three-year commitments in terms of savings, contracts, and reservations. If a consumer registers for Microsoft Azure and agrees to pay for those resources for one to three years, they will receive a discount. However, your reservation will only be valid for the selected resource group.

Additionally, if you commit to paying for these resources for one to three years, Google Cloud will provide you with a discount. On the contrary, when you commit to an instant family, you are dedicated to all its members for the term of the commitment. Unlike Azure, changes or cancellations are not possible. Regarding virtual machines and performance, Google rates 67% among all cloud service providers (CSPs) evaluated by Cloud Spectator, whereas Amazon Web Services (AWS) earns about 75%. Azure is close to becoming the least expensive alternative. In terms of Infrastructure as a service capability and a robust ecosystem, AWS is the apparent victor. Google and Microsoft are exerting significant efforts to remain competitive. Even the top three IaaS providers have dependability and geographical dispersion issues. Amazon's Simple Storage Service (S3) experienced a two-day outage in a North Virginia data center, but only for customers who did not employ multizone storage replication. Internal administrative problems, such as improper router code updates, account for most failures at large providers. They all provide the same services. However, they may differ in minor aspects, such as service standards.

3. For each provider (Amazon, Google, Microsoft), identify specific risks, and prepare to offer specific suggestions for launching, running, and managing the proposed new service if that provider is chosen.

AWS Cloud:

Amazon Web Services will be able to handle practically all financial business requirements, including computer, database, infrastructure management, application development, and security. AWS offers many services, including Virtual Private Cloud, Data Transfer, Simple Storage Service, Elastic Compute Cloud, and Key Management Service.

AWS also provides infrastructure security, DDoS mitigation, data encryption, inventory and configuration, monitoring and logging, and identity and access management. It also boasts over 40 compliance certifications, both globally and domestically.

The risk associated with this service is that it needs to integrate third-party tools. When considering AWS as a provider, we need to check if amazon provides any in-house tools since there are risks associated with using third-party tools, such as loss of support and unresolved bugs.

Advantages:

AWS provides the most services to corporations on a "pay as you use" basis, meaning you only pay for what you use. On their website, there is also a "Free tier service" area where you may join up for a 12-month free offer or locate services that AWS provides their clients for free.

Disadvantages:

Because the client's location governs AWS services, you must thoroughly explore whether features are available in your area. The cost of technical support is likewise relatively high.

Pricing:

AWS operates on a "pay-as-you-go" approach, meaning no long-term contracts or licenses are necessary. The monthly fee is determined by the number of services consumed and hours performed (since Amazon EC2 usage is calculated hourly). However, with so many services available at different prices, finding accurate statistics may be difficult, so it's best to utilize their cost calculator or request a quotation.

Google Cloud:

Google Cloud provides organizations with over 90 services ranging from computing and storage capabilities to analytic and networking solutions. Other Google cloud offerings include G Suite, Google Maps Platform, Google Hardware, Google Identity, and Chrome Enterprise.

Google Cloud Platform (GCP), the smallest of the three platforms, provides a more limited set of services and does not have as many data centers as AWS and Azure. It delivers highly specialized services to customers in three primary areas: big data, machine learning, and analytics, as well as solid scalability and load balancing.

GCP provides several cloud security features, such as Virtual Private Cloud, Data Encryption, Intrusion Detection System (IDS), Data Loss Prevention, Anti-DDoS, WAF, anti-bot, and API protection for web and API.

The risk associated with this service is that the volume discount is not realized. While considering this service, we need to analyze the savings Google provides as the number of customers using the service increases and the volume discount kicks in.

Advantages:

Excellent data analytics and storage capabilities, as well as a plethora of innovative machine learning services. In addition, the Platform may be effortlessly connected with other Google services.

Disadvantages:

Because most apps use Google technology, switching from Google Cloud Storage to another platform might be difficult.

Pricing:

Like its major competitors, Google Cloud provides a pay-per-use basis, with the fee rounded up after every 10 minutes of use. You may either pre-calculate the prices using the Calculator app or get a quotation. New users will also receive $300 in free credits to explore the Google Cloud Platform fully.

Azure Cloud:

Microsoft Azure offers over 200 products and services in areas such as AI and machine learning, developer tools, hybrid cloud, Internet of Things, mixed reality, and networking. Azure may also be easily linked with the rest of Microsoft's products, including Office 365.

Azure provides a unique security solution that adheres to the ADADSC model: detect, assess, diagnose, stabilize, and close. As a result of their strict standards, they have received over 90 compliance certifications for IaaS security.

The risk associated with this service is that it is challenging to customize integration. While considering this service, we need to research customizing configuration to evaluate for better performance and cost savings.

Advantages:

Azure distinguishes itself from its competitors by offering a 99.95% service level agreement (SLA). (Each year, approximately 4.38 hours of downtime) It has the most security certifications of any cloud platform, which is a huge advantage.

Disadvantages:

It isn't easy to establish the Platform's cost because each Azure service comprises supplemental services necessary to perform the services you desire. Also, keep an eye out for hidden expenditures like transfer and backup fees. And, like AWS, their support service is not cheap.

Pricing:

Microsoft Azure pricing is complex due to software licensing as well as the fact that they charge by the minute, with costs stated as hourly rates. If you operate the VM for less than an hour, you will be charged based on the total number of minutes spent. You will also be responsible for any underlying infrastructure resources, such as storage or networking. Requesting a quote to determine the approximate cost of your service is preferable.

Preferred Service:

AWS

Apart from the cloud, fintech firms build on cutting-edge technology such as mobile and blockchain. On the other side, established Fintech firms understand the benefits of AWS cloud owing to its cheap capex cost, making AWS Cloud a very appealing computing infrastructure.

It provides capabilities that include:

Seamless and Safe Transaction Data Backups

Better Performance and Scaling

Supporting DevOps Culture

24 x 7 x 365 Availability

With such exceptional capabilities and complete software development lifecycle assistance from development to deployment, AWS is unquestionably an ideal match for Fintech organizations embarking on the path of digital transformation.

4. Evaluate the strength and weakness of Fintech's provider evaluation process. What useful steps were taken? Do you see any problems?

Strengths of Fintech's provider evaluation include in-house evaluation, defined use cases for evaluation, and major cloud providers specifically being appropriately evaluated in a sort of significant way. The weakness in this evaluation, for the most part, is that the assessment was primarily performed only using the data provided by the cloud service providers in a significant way. The steps generally included in the Fintech's provider are evaluation team basically were briefed on the service requirements and the use cases, guiding principles should be clearly defined, and each cloud service provider should consider the most part be compared under the same criteria tremendously. The only problem involved in this evaluation process would be that each evaluator solely focused on their assigned cloud service provider.

Risk analysis

Vital assets in the organization require protection in business processes (NIST,2011). Assets can be tangible or intangible items that work to achieve Fintech's mission of migrating to the cloud. When assessing importance, we look at investments that pose the highest risks and impact on the organization. At Fintech, there is a critical component related to protecting intangible assets used by all stakeholders, especially regarding financial information and other data for its customers. These assets include software and data used to process finances, such as customer PII, order management software, email, website, etc. These require protection through virtual means to avoid unauthorized access, destruction, and downtime. When protecting these intangibles, physical security still plays be important. Specific measures are also required, such as acceptable use policy, antivirus, cyber monitoring, etc.—ultimately enabling the organization to focus on protecting critical assets that pause the highest risks.

This section identifies the possible security and privacy risks to develop a complete picture of the criteria. Fintech needs to determine the best course of action for choosing a cloud service provider. We applied the operationally critical threat, asset, and vulnerability evaluation (OCTAVE) methodology, known as OCTAVE Allegro (Caralli et al., 2007), to assess this case's privacy and security risks.

The OCTAVE Allegro method focuses on information assets and considers different information containers, such as databases and physical and virtual assets. The fundamental goal of this section is to highlight the various privacy and security vulnerabilities and threats related to Fintech and the three cloud service providers, present the risks, and propose approaches to mitigating the identified risks. We were able to execute this in a 5-step process.

- Step 1: The team identified critical information assets for the organization. The methodology also provides a set of questions and asks, for example, What is the value of assets or the dependency on the asset for the day-to-day business of the organization, both physical and virtual. (See Table 1).

Asset Identification
Reputation Brand
Software and Data ● Customer PII ● Electronic fund Transfer Payment System (EFTPS) ● Email, Websites ● Proprietary Software ○ Local custom packages ○ Database
Third-Party Vendors
Payment Financial Data
Employees

Table 1

- Step 2: Identify Vulnerabilities. This phase aims to identify essential Infrastructure and organizational vulnerabilities that presented themselves in this case (See Table 2).

- Step 3: Threat Identification. The team considered any external circumstance or event that may cause harm to an asset, both passive and active. The results of this assessment involved a structured identification of all potential threats. The analysis included physical hardware assets, productivity, reputation, finances, and fines. It's important to note that when threats exploit vulnerabilities, bad things occur, as indicated in this case. For example, Fintech's exposure to legacy applications and proprietary software, coupled with the threat of data loss and hacked interfaces of APIs, results in the complication of choosing a compatible cloud service provider (See Table 2).

Threats	Vulnerabilities
Data Breach	Infrequent Data backups
Compromised Credentials	Data Integration
Hacked interfaces and APIs	Legacy Applications/Proprietary Software
Cloud Service Abuse (DDoS attacks, APT Parasites, phishing attempts, e mail spam, digital currency "mining")	Separate copies of data requirements
Data loss	
Shared technology, shared dangers	Time constraints for regulations

Table 2

- Step 4: After considering vulnerabilities and threats, the team analyzed controls that were in place to prevent and mitigate risk. Our review considered the safeguards and countermeasures to combat privacy and security concerns (See Table 3).

Threat/Impact Area	Controls
Cloud Service Abuse	Redundancy / Failover System (Route 53)
Hacked interfaces and APIs	Two Factor Authentication
Data Breaches	Data Encryption,
Compromised credentials	Role base access controls (RBAC), 2FA
Data loss	Data Standardization
Shared Technology, Shared Dangers	A framework of security policy for integrato rs

Table 3

- Step 5: For the team's mitigation approach, we used qualitative and quantitative risk assessment methods to examine our identified risk. An example is provided in table 4, which focuses on creating a relative risk score for each identified threat scenario. The impact on each area and the impact area's probability will be reflected in the total risk score. For each impact area, we assigned a value of measure that included low, medium, and high (1-3). Finally, the significant sites will be ranked from high to low based on the likelihood of occurring. We had six areas (1-6). The score allowed us to decide what mitigation approach to choose in the ultimate step of the methodology (See Table 3).

- Pool 1: Accept

- Pool 2: Mitigate

- Pool 3: Transfer

- Pool 4: Avoid

Impact Area (Ranked)	Probability (1: Least – 6 Most Likely)	Business Impact	Value (1-3 Low -High)	Risk Score	Risk Ranking (Decision)
Cloud Service Abuse	6	High	3	18	Transfer
Hacked interfaces and APIs	5	High	3	15	Mitigate
Data Breach	3	High	3	9	Mitigate
Compromised Credentials	4	Medium	2	8	Mitigate
Data loss	2	Medium	2	4	Mitigate
Shared technology, shared dangers	1	Low	1	1	Accept

Table 4

Impact on Systems

Our risk analysis also looked at Cloud Service Alliance (CSA) specific concerns in the cloud in 2016. The table below demonstrates what impact each potential attack can have on Fintech. An attack on Fintech would impact its operations, assets, and the individuals affected. For example, an attack on the EFPTS system would significantly affect Fintech's operations. It would cause a stoppage of all transactions until the issue is resolved. Fintech will not be able to conduct operations until this issue gets resolved successfully. This attack would create negative attention for Fintech, causing a considerable loss of customer trust and reputation damage. Most importantly, this would potentially cause severe financial disruption for Fintech.

Additionally, as seen from other historically significant cyber-attacks on companies such as Target in 2014, individuals would also be affected by an attack on Fintech's EFPTS system. EFPTS systems store a lot of customers' information. They contain card information, as well as personal information. If an attacker successfully gets this information, it can be sold to people on the Dark Web in bulk. This could lead to future lawsuits for Fintech after the stolen cards are used fraudulently. Additionally, the breached EFPTS systems might suffer permanent damage if not appropriately recovered. Although unlikely, this could lead to a loss of data and/or access to the EFPTS systems.

Type of Impact	**Possible Outcomes**
Operations	• Disruption to future business operations • Loss of Customer trust • Financial Loss • Reputation Damage
Assets	• Damaged EFPTS system • Loss of Data • Loss of access to EFPTS

Individuals	• Stolen PII Data • Lawsuits • Fraudulent Payments

Weighted Factor Analysis

Threats:

Criteria	**Criterion 1: Frequency of Attack (0-1.0)**	**Criterion 2: Reputation loss if successful (0-1.0**	**Criterion 3: Financial loss if successful (0-1.0**	**Weighted score**
Criterion Weight (1-100)	20	45	35	100
Cloud service abuses	*0.4*	*0.8*	*0.7*	*68.5*
Hacked interfaces and APIs	*0.8*	*0.6*	*0.5*	*60.5*
Data Breach	*0.5*	*0.5*	*0.4*	*46.5*
Shared Technology, Shared Dangers	*0.2*	*0.4*	*0.5*	*39.5*
Data loss	*0.3*	*0.4*	*0.4*	*38*

After performing a weighted factor analysis for the possible threats to Fintech's migration to the cloud, we concluded that the top 3 weighted score prioritization is; Cloud service abuses (Phishing attacks, DDoS Attacks, email spam), Hacked interfaces and APIS, Data Breaches. While Cloud Service abuse attacks have the lowest frequency and possibility of happening, if it does happen, they would still have a severe impact that it retains the highest weighted score on our WFA.

Assets:

Criteria	**Criterion 1: Impact on revenue**	**Criterion 2: Impact on profitability**	**Criterion 3: Impact on public image**	**Weighted score**
Criterion Weight (1-100)	35	25	40	100
Reputation/Brand	.8	.8	1.0	87
EFTPS System	.8	.7	.2	54.5
Customer PII	.7	.5	.5	54
Proprietary Software	.8	.5	.3	49

After performing a weighted factor analysis for the assets that Fintech has related to concerns for cloud migration, we concluded that the weighted score prioritization is; Reputation/Brand, EFTPS System, and Customer PII data. Reputation/Brand for Fintech is the most critical asset according to the weighted score we assessed.

Risk Determination

Once a threat's probability of an attack has been evaluated, the organization will typically look at the possible outcomes or consequences of a successful attack. The results of an attack (often as a loss in asset value) are of great concern to the organization in determining where to focus its protection efforts. Most commonly, organizations will create multiple scenarios better to understand the potential loss of a successful attack, using a "worst case/most likely outcome" approach. It is helpful for organizations to retain this information, as it can also be used during contingency planning. If an existing control fully manages a vulnerability, it can be set aside. If it is partially controlled, we can estimate what percentage of the exposure has been controlled. In this case, we use a few scenarios of mitigation controlled by Cloud Service Providers to look at risk ratings.

- Cloud Service Abuse: (L*I)-M%+U% = (0.8 * 75,000) - 0% +10% = **$66,000**
- Hacked interfaces and API: (L*I)-M%+U% = (0.8 * 55,000) - 0% + 10% = $**24,200**
- Data Breach: (L*I)-M%+U% = (0.5 * 55,000) -0% + 10% = **$30,250**
- Shared Technology, Shared Dangers: (L*I)-M%+U% = (0.2 * 45,000) - 0% +10% = $**9900**
- Data loss: (L*I)-M%+U% = (0..3* 40,000) -0% + 10% = $**13,200**

Cost Benefit Analysis

To complete the cost-benefit analysis, the Annual Loss Expectancy (ALE) before and after the controls are implemented are taken into consideration. The cost to successfully implement the control is also factored into this calculation. For Fintech, since Hacked interfaces and API is the most considerable risk, we looked at all three cloud service provider choices. The values derived are from Exhibit 8 Monthly Cost Estimates for each provider.

Controls

1. AWS for $19,656 annually, which reduces SLE by 25%
2. Microsoft Azure for $87,612 annually, which reduces SLE by 25%
3. Google Cloud for $20,208 annually, which reduces SLE by 20%.

CBA = Present Value of Future Benefits / Present Value of Future Cost

- **AWS: 2.52**
- Microsoft Azure: **0.80**
- Google Cloud: **2.46**

Recommendation

Because of the low related capital expenditure costs, established fintech businesses will benefit from the AWS Cloud, making the AWS Cloud a very appealing computing platform.

The top five reasons to utilize the AWS cloud, whether you're an IT decision-maker or a DevOps worker at a fintech organization, are listed below.

1) Compliance and regulations in one click

Security is the number one priority in the AWS Cloud. AWS users can benefit from a network and data center architecture designed to meet the needs of the most security-conscious organizations. AWS Cloud Compliance helps customers understand performance controls. Additionally, AWS offers a 3-tier web architecture training model, demonstrating integration with multiple VPCs for security and privacy in the cloud. Deploy secure architectures quickly and easily with AWS cloud profiling tools. AWS controls the security of our cloud infrastructure, but we are still responsible for the security of the applications that run on AWS. You can manage security measures to protect your platforms, applications, systems, and networks

2) Fast and secure transaction data backup

Transactions are the basis of banking and finance. The transaction data generated must be stored and securely stored for later retrieval. Transactional databases should be kept in different geographies based on disaster recovery requirements. In addition, procedures must be in place to ensure a quick recovery during an interruption. AWS's robust disaster recovery (DR) policies make this easy. One of the critical use cases for cloud platforms like AWS is highly secure, fault-tolerant disaster backup and recovery.

3) Scalability and performance

The majority of fintech companies are consumer-centric or B2C. To meet this need, AWS provides auto-scaling features that help maintain service continuity during peak hours. You can increase Amazon EC2 instances dynamically to maintain performance during peak hours and reduce capacity during off-peak hours to save money.

4) Available 24 hours a day, seven days a week, 365 days a year

With the democratization of mobile phones, the services of fintech companies need to operate 24/7, 365 days a year, so that customers can access their services anytime, anywhere is clear. AWS Auto Scaling helps FinTech organizations maintain application availability and enables customers to dynamically scale up or down their AWS EC2 capacity based on usage trends.

5) Encourage DevOps culture

Rapid delivery of new products is one of the key value propositions for fintech companies. For rapid deployment, fintech companies must adopt a DevOps approach. AWS supports DevOps by providing a complete toolchain available. This AWS DevOps toolchain includes AWS Code Commit to private git hosting of your codebase and AWS Code Pipeline continuous delivery service to automatically develop, test, and deploy your code to any instance EC2. AWS to automate the deployment of your code which includes Code Deploy any EC2 instance.

Conclusion

The cloud is nothing new to the fintech industry. Cloud-based solutions have become the standard for many financial organizations over the last decade due to enhanced storage and security capabilities and the cost savings associated with no longer operating on-premises data centers. Still, as the industry has changed and the needs of fintech applications have expanded, new requirements have emerged, such as better scalability, always-on dependability, outage-proof performance, and global deployment capabilities.

Cloud-native apps are created, designed, and maintained on the cloud. Because the architecture is fundamentally cloud-based, these apps make deploying new features and solutions more manageable. On the other hand, programs in a normal cloud-based environment exist in on-premises applications that have been migrated to the cloud but have not been optimized for the environment. Because of the always-on, fast-paced nature of transactions, the subtlety of cloud-native is critical for Fintech.

While cloud-native is now the best option for Fintech, we all know that change is unavoidable. Looking ahead, the necessity for a poly-cloud or multi-cloud environment in the fintech industry is anticipated to grow. Three primary considerations will drive this shift: consumer preferences, dependability needs, and application development optimization.

Often, fintech consumers prefer which cloud service handles their data. As a result, fintech providers will need to create apps that can function natively across numerous cloud infrastructures.

Similarly, when fintech firms extend their operations, providing fail-safes across cloud platforms improves service dependability. Finally, financial firms will seek to employ several clouds to construct specific application components. Companies may optimize application development for the most significant user experience by leveraging the characteristics of each cloud platform.

References

Fields, D. (2022, April 19). *Why the future of Fintech is cloud-native*. Spiceworks 1. Retrieved December 8, 2022, from https://www.spiceworks.com/tech/cloud/guest-article/why-the-future-of-fintech-is-cloud-native/#.

Jakub Skowron in FinTech Business, About the author Jakub Skowron Technology enthusiast, author, A. the Jakub Skowron Technology enthusiast, Skowron, J., & enthusiast, T. (2022, July

1). *Top 3 cloud services providers for FinTech*. Code & Pepper. Retrieved December 8, 2022, from https://codeandpepper.com/top-3-cloud-services-providers/

Caralli, R., Stevens, J., Young, L., & Wilson, W. (2007). The OCTAVE Allegro Guidebook, v1. 0. Cert Program, Software Engineering Institute. In: Carnegie Mellon University, Pittsburgh, PA.

Huth, A., & Cebula, J. (2011). The basics of cloud computing. *United States Computer*, 1-4.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

Appendix

Exhibit 5: Fintech Architecture Diagram

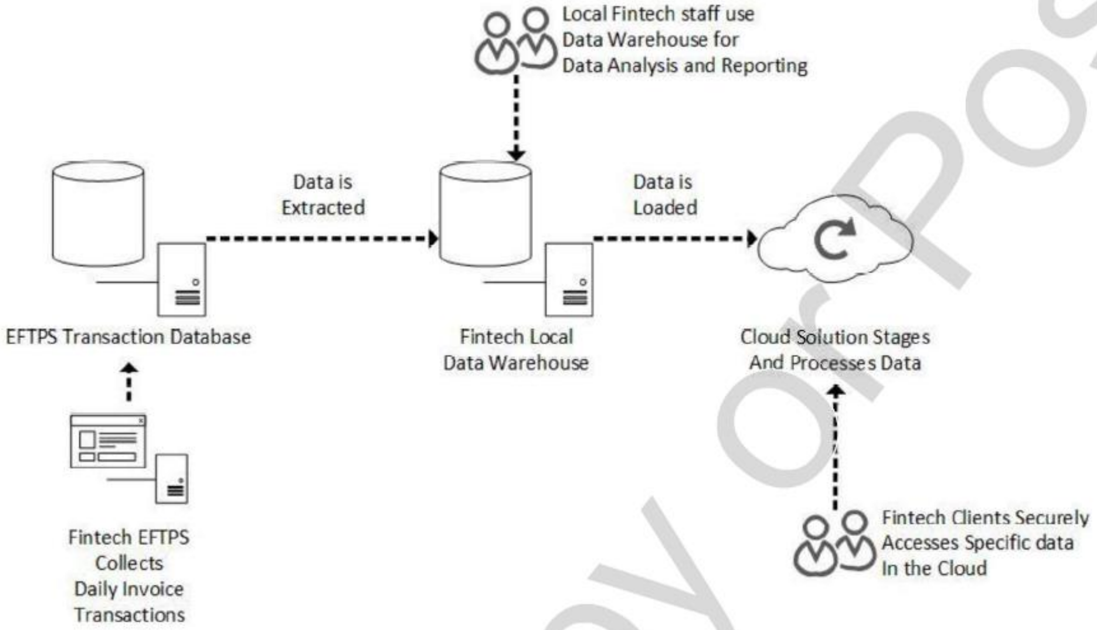
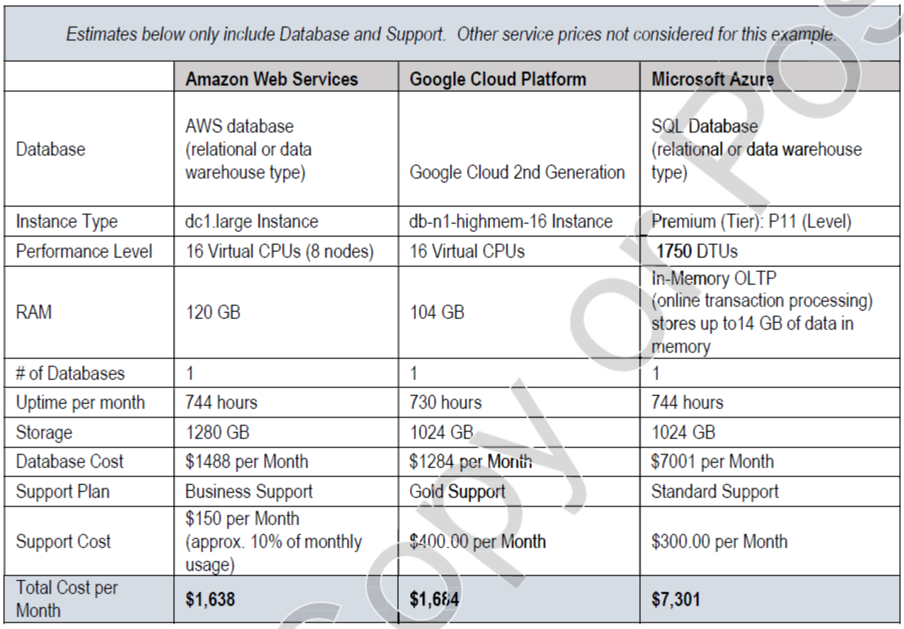


Exhibit 8: Monthly Price Estimates for Use Case

(Price estimates calculated applying each vendor's calculator to the Use Case).



Estimates below only include Database and Support. Other service prices not considered for this example.

	Amazon Web Services	Google Cloud Platform	Microsoft Azure
Database	AWS database (relational or data warehouse type)	Google Cloud 2nd Generation	SQL Database (relational or data warehouse type)
Instance Type	dc1.large Instance	db-n1-highmem-16 Instance	Premium (Tier): P11 (Level)
Performance Level	16 Virtual CPUs (8 nodes)	16 Virtual CPUs	1750 DTUs
RAM	120 GB	104 GB	In-Memory OLTP (online transaction processing) stores up to14 GB of data in memory
# of Databases	1	1	1
Uptime per month	744 hours	730 hours	744 hours
Storage	1280 GB	1024 GB	1024 GB
Database Cost	$1488 per Month	$1284 per Month	$7001 per Month
Support Plan	Business Support	Gold Support	Standard Support
Support Cost	$150 per Month (approx. 10% of monthly usage)	$400.00 per Month	$300.00 per Month
Total Cost per Month	**$1,638**	**$1,684**	**$7,301**