IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91223

Leveraging Cloud Infrastructure for Scalable and Secure Digital Finance Ecosystems

Murali Malempati

Senior Software Engineer, mmuralimalempati@gmail.com, ORCID: 0009-0001-0451-9323

Abstract: Digital finance encompasses digital information feedback on credit credibility and electronic transactions based on digital currencies. In recent years, driven by blockchain technology and cloud computing, digital finance has boomed in developed countries, giving rise to new issues and potential risks. With the transformation of digital finance from 'crypto' to 'cloud', a new trend is emerging. Digital finance driven by cloud computing, whether on public clouds or on-chain clouds, offers a plethora of opportunities, but the migration to native digital finance systems based on cloud infrastructure would be fraught with risk. Cloud computing, with its convenience, flexibility, security and scalability, continues to become a mainstream technology in retail finance. Multi-modal federated machine learning and federated cloud transactions can potentially construct a decentralized market with permissioned access while achieving snapshot privacy. Blockchain will continue its widespread adoption in developer-centric financial backends as technology matures, with larger public chains evolving to handle benchmark trading volumes. On miniambilest, native public and enterprise banks, decentralized exchanges, NFT-backed loans and on-chain credit scores will rise, creating liquidity for illiquid assets and granting borrowing access to previously excluded participants. The rising popularity of cryptocurrencies may, on the contrary, accelerate KYC, AML and the adoption of CBDCs.

Security issues in cloud computing may cause significant financial losses, as there have been cases in the past where public cloud services have suffered data breaches. In some cases, thousands of GB of customer financial and transaction data have leaked online and caused significant reputational damage, emphasizing the importance of choosing a reliable cloud service vendor [2]. Observations made during web scraping consisting of an analysis of exchange user cases showed that data breaches have exposed customer account information, previous transactions, and even 3D model photos of the vault and keys used to hide hardware wallets in a bank deposit facility. Furthermore, the archive and backup of large-scale retail finance databases in the public cloud may incur long data retrieval delay of over 100ms. The lost backup can also put the entire institution at risk if the vendor service becomes bankrupt, or if a natural disaster damages their facilities. Despite the rapid year-on-year growth of this new financial market, currently, only limited assets, such as the Bitcoin reward for blockchain mining, can be traded on-chain.

Keywords: Cloud Computing,Digital Finance,Scalability,Cybersecurity,Fintech Infrastructure,Cloud Security,Financial Technology,Hybrid Cloud,Data Encryption,Regulatory Compliance,High Availability,Multi-Cloud Strategy,Digital Transformation,Infrastructure as a Service (IaaS),Real-time Data Processing.

I. INTRODUCTION

The outbreak of COVID-19 variants has further triggered rampant infections across the globe, and SMEs have again suffered economically due to delayed payments from clients, falling sales, reduced liquidity, and enormous losses. At present, there are nearly 50 million SMEs in China, which means a huge capital demand in this segment, and it is also a mass pain point as the traditional banking industry is reluctant to dig deep into SMEs. Cloud computing, the on-demand delivery of IT resources over the internet with the pay-as-you-go pricing model, is profoundly changing the landscape of the financial industry. As the foundation of fintech, advanced cloud infrastructure helps increase the number of online infrastructures and the elasticity of scaling up/down computing efficiently. Traditional banks are also actively embracing cloud computing with versatile options such as public, private, hybrid cloud, multi-cloud, or on-premise modes to transform their legacy infrastructure, improve service resiliency, alleviate on-premise maintenance burdens, and achieve compliance. In 2024, global public cloud spending is projected to reach $657 billion, an increase of 23.1% from 2023, still growing faster than gross domestic product estimates.

The ability to circumvent traditional on-premise infrastructure drawbacks and provide instant access to scalable and secure financial services positions cloud computing as a springboard for accelerating the digital evolution of the traditional finance industry. This paper aims to address the burgeoning need for a secure and scalable cloud infrastructure for digital finance. Drawing inspiration from traditional finance, the layering approach with backends for resilience and security, the front-end for high performance in increased availability and latency targeting worldwide clients is introduced

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91223

to assist in the architecture design. Furthermore, the design considerations focusing on scalability and security assurance are elaborated upon concerning the rapidly evolving requirements of the digital finance sector. Digital finance has fundamentally transformed the traditional financing ecosystem through advanced technologies in intelligent digital identities, the blockchain-based decentralized ecosystem, and cloud computing.

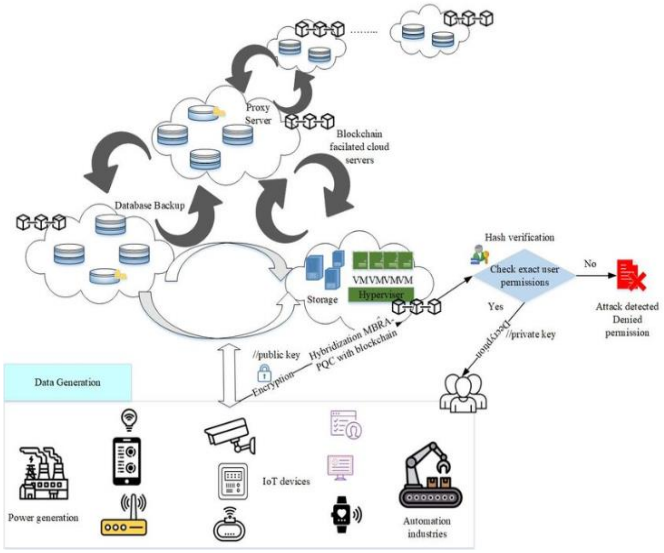

Fig 1: Cloud Infrastructure for Scalable and Secure Digital Finance Ecosystems

1.1. Background And Significance

The author presumes that financial technology (FinTech) is an important burgeoning industry for future growth. Digital strategy in Finance can be considered the growth strategy of the future for finance-related companies, such as banks, securities, trusts, shipper brokers, insurance, etc. Capturing the unique features of the financial industry is crucial for FinTech start-ups to target market players and determine their business model and strategy. Digital strategy generation will be a collaborative effort with financial industry experts and analysts. Literature on digital strategy in finance is sparse, as it is an emerging area of research. The concept of the digital strategy in finance that focuses on FinTech companies is first introduced. The empirical study shows the unique features of finance-related industries that form a foundation for strategy generation. Furthermore, the author proposes strategic pathways for digital strategy adoption, implementation, and capturing expected gains. This study demonstrates the direction of development for accelerators and VC companies interested in the FinTech industry and guides banks, securities companies, and other financial industries in shaping their digital strategy. Digital finance (DF), which is characterized by a great leap forward in service efficiency and inclusiveness on the basis of digital technology, is currently at the core of the financial development strategy of most countries, while SMEs have become one of the key supports for national economic development. The rapid development of digital finance has brought novel choices and changes to SMEs financing, and the information cost and transaction cost associated with financing will be reduced. However, the digital divide in a great many countries remains an issue, which alarms to investigate further whether digital finance can reduce the difficulties of SMEs financing in the developing country context at large. The author posits that digital finance can promote financing accordingly by alleviating the information opacity. Furthermore, since the impact of digital finance on SMEs financing is a multi-facet and long-term process, the distinguishing impact on each of the attendant avenues has been elaborately examined. In order to formulate the richer policy recommendations based on the heterogeneous responses of SMEs groups with varied characteristics to digital finance, the emphasis is put on the motivation for heterogeneous influence.

Equ 1 : Cost Optimization Equation

$$\text{Total Cost}_{cloud} = \sum_{i=1}^{n} (U_i \cdot R_i) + S + M$$

- U_i: Usage of resource i (e.g., CPU hours, storage, bandwidth)
- R_i: Rate per unit of resource i
- S: Cost of security measures (e.g., encryption, monitoring)
- M: Management/operational overhead

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91223

II. UNDERSTANDING CLOUD INFRASTRUCTURE

Considered to be the most prominent change since the advent of the Internet, Sustainable Cloud Computing aims to tackle the problems of the original model of Cloud Computing, building on top of it and preserving its advantages. Cloud Computing refers to the service-oriented delivery and renting of computing resources. The service-oriented delivery of resources allows on-demand provisioning and an unprecedented level of scalability for customers. In this relationship, customers give their control over computing resources which is then assumed by Cloud Providers. Thus, customers hand over their data and application control to the Cloud Providers. Such transfer of control over sensitive data and applications is referred to and equated to a loss of data sovereignty. Data security is a complex question that, while hardly an everyday consideration, has an influence on the conduct of day-to-day life. Data sovereignty can be viewed from many different angles. With its omnipresence, the Internet is thoroughly engraved into everyday life. Inextricably it has changed the way people conduct their professional and private lives. Digital Financial Services on-premises facilitators, such as Banks, Mobile Network Operators, etc., are juxtaposed with Over-the-top players providing Digital Financial Services such as mobile money; many of whom do not have regulatory or consumer protection oversight.

Security, privacy, and compliance breaches, as a rippling effect of the openness of many Cloud services, are still common occurrences today. These may not only result in loss of sensitive data such as account login information and health records but may also result in the direct monetary loss of a few decimal places in the bank account through sophisticated breaching techniques. Industries tried to build private Clouds internally as a means to reduce reliance on external Cloud Vendors but quickly fell back to public Clouds as the costs and efforts to maintain such infrastructures was found to be unsustainable. Hybrid Clouds were adopted. Two different types of deployment Cloud models are public Clouds owned and operated by one organization and offered to the general public for a fee and private Clouds owned and operated by one organization and dedicated to it.

2.1. Types of Cloud Services

In addition to rich Internet applications, cloud computing facilitates new classes of applications that would not have been possible otherwise. These cloud-based applications require the application and associated data sets to be hosted online. The entire combination is referred to as a cloud service, which represents a new online service with at least one of its functions implemented as an emerging cloud computing model. In a cloud computing system, there's a significant workload shift. Local computers no longer have to do all the heavy lifting when it comes to running applications. The network of computers that make up the cloud handles them instead. The reverse is true for the cloud's central computers, which will have to do much more as they handle the bulk of computational requests. As a result, the computational demand becomes much higher in the cloud. One result is a reduction of hardware and software demands on the user's side. The only thing the user's computer needs to be able to run is the cloud computing systems interface software, which can be as simple as a web browser. Generally, there are three common types of clouds available: Private cloud, Public cloud, and Hybrid cloud. A Private cloud has been based upon a pool of shared resources, whose access is limited within organizational boundaries. The resources are accessed over a private and secured intranet and are all owned and controlled by the company's IT organization. A Public cloud, in contrast to a Private cloud, is a domain where the public Internet is used to obtain cloud services. In this manner, the owner of the cloud provides its resources and services on a pay-per-use basis to customers, in turn, leveraging the economies of scale in a highly economical and efficient manner. A Hybrid cloud is a combination of private and public clouds. The two domains are interconnected by standard technology, which enables consuming services from each domain in an integrated fashion.

Currently, the industry has also been successfully adopting three common types of cloud computing service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS is a service model around servers, storage capacity, and network bandwidth. The data is relevant to the end-user, but the underlying OS and applications, even backup, are implemented and managed in the cloud provider's infrastructure. The service provider is responsible for providing server configuration and maintenance, network topology, and storage configurations, and the cloud user can use the cloud to scale computational resources on demand. PaaS, like IaaS services, provides an externally managed platform for building and deploying applications and services. Runtime management, scaling, deployment, high availability, and fault-tolerance are all supplied in a fully managed way, which also frees cloud users from maintenance and performance concerns. In a way of least user concern, the cloud feels like an on-premises environment. Logically, all the resources still belong to the user, and the user is only responsible for code, environment, and services deployed to the platform. SaaS is simply having a software system running on a computer that does not belong to the customer. Business-wise, the cloud provider is capable enough to host and maintain a software system that can provide a wide coverage of potential end-users.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91223

2.2. Key Cloud Providers

This section describes key cloud providers, providing the background of the top-tier of public cloud providers, focusing on those with Asian backgrounds, including AWS, Azure, and Aliyun. The ranking of the cloud service providers is according to company revenue announced publicly per last calendar year, from which the sum of the total provider's revenue worldwide is estimated. The numbering of the cloud service providers is enumerated based on the value of company revenue, not in the signifying value by the company name.

Not only does AWS top the cloud provider market share by revenue, but it is also one of the cloud providers that leverage the most data. Most data uploaded to AWS are of the cloud-native service type, which is either built with proprietary technology or open-sourced technology and built on EC2. The average situation of data leveraged by AWS cloud storage service is shown from the aspect of distribution ratio yearly.

Aliyun, known as Alibaba Cloud or Aliyun, is a Chinese cloud provider founded by Alibaba Group, whose E-commerce business and payment service have already been adopted by an enormous number of people in China and Asia. Compared to AWS, the speed of Aliyun taking off is even faster, as it was founded in 2009 while AWS has already existed for years. It is shown that 64% of users leverage only one cloud storage service, while Aliyun is the most common with almost 40% lone users. AWS and Google both have around 20% lone users, which suggests that they start leveraging cloud services later than other users. Meanwhile, as time goes on, the chances for the current lone users to adopt an additional cloud provider are still rising, indicating continued growth in the server industries.

Microsoft Azure is the ISV platform from Microsoft, which is also an infra provider. Compared to AWS, the IaaS services of Azure were released a little later. Azure builds up the service layer slowly, but it does a good job in the application layer where countless productivity enterprise software build on it. Once an enterprise adopts Microsoft software in office, CRM and ERP, it would be very easy to leverage Azure services to meet their cloud computing needs of web services. Another aspect is focused on those using the combination of cloud storage services. It is observed that, while Aliyun users will likely adopt UCloud, AWS users would likely adopt GDrive. This infers that AWS and GDrive might be competing with teams to attract users from a group of bigger cloud service providers.

2.3. Cloud Architecture Basics

Cloud computing comprises a service-oriented computing paradigm in modern information technology arcs. This off-site calculation model, managed and maintained by service providers, can be blended based on public resources or private enterprise resources. The resources can be elastically and online requisitioned based on service demands via networks. Typical basic service modes include: 1. Infrastructure as a Service; 2. Platform as a Service; and 3. Software as a Service

In the cloud computing model, personal digital devices, normally low cost, will be used to access all kinds of software services on the Internet via networks. Important features of this computing model include: 1. High degree of integration of resources. In the cloud model, a computing SW/HW system is normally made up of a data center where resources of network, server, mass storage, and power supply can all be integrated and reallocated. The resource integration will enable a super computing power and a great capacity of IT applications. 2. Strong impact resistance. Unlike the off-Internet computing mode, information can be stored in many backup copies on different servers in a data center, thus the loss of cloud data can be minimized even when some nodes are broken or crashed. 3. High scalability of service. A cloud system is normally made up of many commercial server units, thus a more powerful computing system can be constructed simply by involving more server units. 4. Low use cost. Generally, the occupant of a cloud itself will bear basic loading costs of the data center, therefore the demand side can save a great expenditure on buying full computing items. As time goes on, it will reduce the use cost for each application.

The cloud platform adopts distributed data storage to store data in a professional data center which consists of many hard disks in adjacent servers for improved security and resource utilization. Prices of cloud data storage charged by unit space and using period are lower than local hard disk devices. The data will be retained in the cloud platform until verified deleting requests are issued and processed. Data requests are normally processed by web-based interfaces, which can be used to upload, download, edit, and share documents. An encrypted channel and query keywords are usually used to protect personal data privacy. Basic encryption methodologies include symmetric-key and public-key encryptions, which can be used flexibly to protect the authentication of both sides in a cloud service. The modular design of the cloud platform enables users to add those extended devices easily, and permit associated devices to be used seamlessly. Such modular design also makes the user level cost lower than otherwise investing in standalone devices.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91223

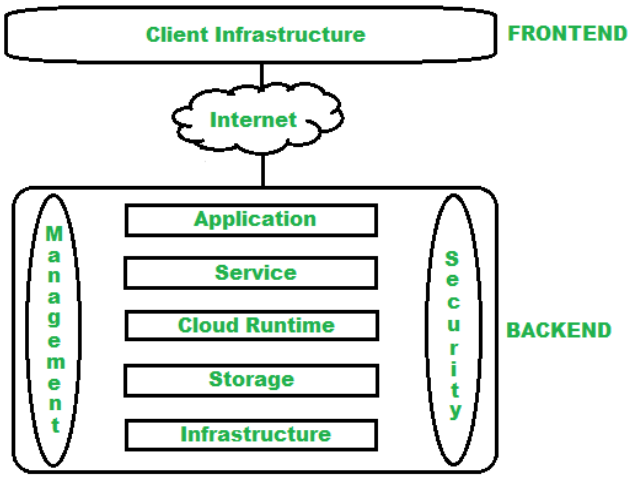

Fig 2: Architecture of Cloud Computing

III. DIGITAL FINANCE ECOSYSTEMS

Digital finance ecosystems are rapidly developing on a global scale, with a diverse range of entities, including banks, fintech companies, pharmaceuticals, technology companies, and telecommunications operators, leveraging innovations in cloud computing, artificial intelligence, big data, blockchain, and the Internet of Things to explore new technology and business models that can provide digital finance services across industries. However, designing, constructing, and managing complex digital finance ecosystems that integrate heterogeneous participants and services in a seamless, secure, and scalable manner represent significant challenges. Evolving cloud architecture that is scalable, highly available, redundant, secure, and capable of federated control to satisfy the needs of digital finance service providers and customers can help significantly facilitate and develop these ecosystems.

Cloud infrastructure and services are critical enablers of emerging mass information and digital ecosystems. In particular, compute, storage, and network resources and services that can be incrementally added, reconfigured, and easily made available to different participants are essential for enabling scalable multi-party systems. The cloud resource pool must ensure appropriate redundancies and backups, and provide highly available services to ensure a seamless experience for digital finance customers. Multi-layered security services, including consistent monitoring of cloud services such as access control, encryption, and federated governmental control, are essential for making customer information and services on cloud infrastructure secure. It is also necessary to design and implement a platform that enables interoperability between various service providers, allowing them to be integrated into a seamless ecosystem.

To address the above issues, a federated cloud infrastructure is proposed. The architecture of federated cloud infrastructure can be structured into several layers, including a public-cloud-based core federation, a private FIC for one or several banking institutions, and a set of regional or service-based private resource pools owned by cloud partners. Security and governance services can be deployed at each cloud layer to protect security and ensure compliance of outsourced data and services. To facilitate the federation of cloud infrastructure, a three-layer architecture and a set of models and protocols for resource access, scheduling, and monitoring are proposed. The architecture with this set of interfaces provides a well-defined service boundary that can be realized with various implementations, allowing diverse resource providers to act as federation partners seamlessly.

3.1. Definition and Components

Digital finance is a financial activity based on digital outputs that is organized through cloud computing services. Digital finance services must ensure asset, privacy, and market security for customers. These services must also meet the availability, scalability, and cost-effectiveness requirements for service providers. Digital finance ecosystems are solutions based on a network composed of providers, customers, and regulators, which provide comprehensive financial services. They can be constructed with a cloud infrastructure consisting of several data centres and cloud edge nodes. Cloud infrastructure is a general-purpose system that can host various applications from providers, and it is formed through cloud computing, storage, and networking technologies. Cloud computing comprises service deployment environments and services. Digital finance ecosystems are provisioned using multiple resources. Cloud-native technologies provide the best platform to construct such ecosystems.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91223

Digital finance consists of a collection of services that provide financial activities for digital assets. In a digital finance ecosystem, there are three peer entities: providers, customers, and regulators. Providers are entities that publish services and honour commitments on a service level agreement. Customers are entities that consume services on a pay-for-use model. Regulators can oversee the operation of an ecosystem to mitigate systemic risks. A global digital finance ecosystem provides services to customers in the economic sector to fulfil digital financial activities across regions. Core services may include payment, exchange, and investment services, which are provisioned using hybrid resources that comprise public, private, and edge cloud infrastructures. Cloud edge nodes hosted in the same district as customers can provide high availability and low latency, while hybrid multi-cloud resources can achieve a balance between data privacy and cost-effectiveness. Services from providers must satisfy customers and meet commitments on availability, delay, and throughput. Customers must also protect their privacy and data security in the ecological environment. Regulators need to ensure lawfulness, dependability, and fairness in such a complex environment.

3.2. Trends in Digital Finance

The evolution of mobile communications and technologies has paved the way for the generation of digitisation potentials in finance and the emergence of digital finance (DF). Over the years, the digitalisation of finance has hastened the transformation of shops into purchasing points, money management behaviours, investors, capital markets, accounting, auditing, tax collection, asset transfer processes, personal finance behaviours, and the investment ecosystem. Apart from the Internet and digital technologies which enable new consumption patterns and payment behaviours, continuous technology innovations in transactions ledgers, smart contracts, and encryption principles have formed new types of currencies and provided automated means of finance. Even in an economy where its fundamental financial services were weak, unreliable, and untrustworthy, no banking services were provided or delivered, there was no stable fiat currency for saving, value keeping, and payment purposes. As a result, in most economies, the informal sector flourished and crypto coins became the only basis for finance. Finance is now described as “digital” in the sense that its infrastructure, content, exchange, auditing, risk monitoring, and audit information have been digital. With the provision of traditional banking services, digital channels, alternative means of payment, their functions and meanings, usability, and how they affect financial behaviours, trust, and the financial information landscape, there are multiple channels for finance.
Digitalisation trends raise awareness on a variety of usages of finance, varied interpretations of trust, and trust-based behaviours. Knowledge has been amassed on the usage of finance in developing economies where essential financial services are missing and absent, based on research methodology that analyses millions of pages collected from browsers and assessment of operational indicators of cashless payments and their impact on banks. Most of the predictions of the potential of digital finance were right, and the evolution of digital finance has begun to transform the financial information landscape, service providers, means, behaviours, risks, and equipment.

3.3. Challenges in Digital Finance

Ongoing tensions among the stakeholders in the digital finance ecosystem could be crystallized into the following challenges : 1. Competition for Digital Finance Users: As multiple digital finance providers spring up to compete for users, customers who were initially happy with the service offered will eventually leave to use a competitor platform if they feel that they are being taken advantage of. 2. Exploitation of Digital Finance Users: As the conflict of interest shifts towards competition among digital finance providers, the top management will have to make decisions that create better value for digital finance users. Digital finance users can get better value if there are strong institutional and legal systems that protect customers from exploitation. Such systems can limit the ability of digital finance providers to pursue excessive self-interests aimed at maximizing profit at the expense of users. Having such systems can lower the incentive of for-profit providers to seek massive profits from serving the poor. 3. Risky Customers: One problem associated with Fintech platforms is that they often attract high-risk customers that conventional banks perceive as risky. Over time, excessive patronage of Fintech providers by risky customers can threaten the stability of financial intermediation if massive defaults arise. 4. Technology and Regulatory Costs: Fintech providers could help reduce the cost of financial intermediation, but technology adoption, online security, and regulatory costs would limit the reduction in the costs of intermediation. 5. Sustainability: The sustainability of Fintech firms in the long run is an important issue for digital finance. Fintech providers typically provide their service for free or for a negligible amount. As margins deteriorate, some analysts suggest that Fintech platforms could turn to ‘data monetization.’

Fig 3: Challenges in Digital Finance

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91223

VI. SCALABILITY IN CLOUD COMPUTING

The rapid adoption of Cloud computing and cloud-based applications has resulted in the emergence of vast and diverse data centers that span thousands of servers, disks, and switches, and capable of storing Zettabytes of data. Searching, browsing and retrieval of such vast quantities of information is no trivial task and brings its own challenges. To improve the extraction of useful data from big data and to reduce the resultant data traffic associated with its transmission, pre-processing and summarization of the information at source is needed.

The scalability of cloud-based services is critical to both data growth and data access. Services must be scalable in terms of data loads, reasonably priced and provide acceptable response times to requests. With regard to cloud performance and service scalability, there is a lack of information about the performance and scalability of already deployed production-style systems. This study demonstrates how modern digital library services can employ CaaS (Cloud as a Service). The cloud should accommodate automatic scalability by reducing the need for fixed server capacity and set-up/storage costs. Well-defined and standard interfaces should be supplied by the service that allow for easy usage of the services. New functions and features are typically embedded in the whole service with the potential risk of adding bugs to already functional components and this may affect the overall performance of the services. This study provides a new architecture with regard to cloud-based co-harvesting and service provisioning.

The system is built with certain key innovative design features. A digital library ecosystem suite of components that work with any underlying digital library content repository. A middleware service for managing cloud services and digital library services. All data communication and movement are done in a safe manner with no direct electronic door for potential manipulation by malicious agents.

Through this service, it will be easier to manage a cloud-based digital library system in terms of international partnerships' services and infrastructures between libraries and organizations, open access resources, costs and expenditure. It provides a scaffold housing for applications and services offered to users. Various services such as data indexing, annotation and linguistics are accommodation requirements and design features of this cloud-based discovery service. Furthermore, these services would automatically scale as needed following instance triggers on preset thresholds to ensure smooth provision of access without compromising performance of the service even in the event of data load spikes.

4.1. Vertical vs Horizontal Scaling

Distributed systems need to be scaled up or down during operation to meet workload changes. Scaling can be achieved by adjusting resources and/or deploying additional instances of the service. Depending on the change type, change duration, and data shareability, distributed systems can be scaled horizontally (scaling out) or vertically (scaling up). Scaling Out involves adding more resources. A distributed Service can be replicated among several machines in a M-to-N manner, where one site handles one service instance only (N-to-1) or each site handles a distinct service instance (1-to-N). Scaling Up involves increasing the capacity of existing resources.

Despite being able to provide additional capacity swiftly, vertical Scaling involves downtime and cannot be adopted with increased loads of a sheer amount. However, where replica sites process similar and, although slightly different requests, horizontal Scaling is put into consideration.

Vertical scaling refers to scaling by increasing the resources of the running service instances. Vertical scaling of cloud applications becomes simpler because all applications run in the same virtual machines instead of having many physical servers. Besides, vertical scaling can dynamically adjust performance cost without complex reconfiguration of load balancing. However, vertical scaling is limited to certain resource capacity and usually leads to service interruption. Furthermore, vertical scaling is less effective than horizontal scaling for all application load scenarios.

Horizontal scaling (or scaling out), on the other hand, refers to scaling by adding a number of duplicated service instances into the system. Cloud platforms usually provide size-supported machines, and a service can choose several machines off-the-shelf. In cloud applications, it is often more efficient to have multiple replicas on separate servers to immediately accommodate a larger scaling up request by newly starting certain running instances. Horizontal scaling usually enables service elasticity, minimizes service interruption time, and has less resource waste. However, it is much more complex than vertical scaling, especially for NoSQL distributed storage systems.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91223

Equ 2 : System Scalability Equation

$$S_{scale} = \frac{R_{peak}}{R_{base}} = \frac{\text{Resources at peak load}}{\text{Resources at baseline load}}$$

- S_{scale}: Scalability factor
- R_{peak}: Resources used during peak demand
- R_{base}: Resources used at normal demand

4.2. Auto-Scaling Features

In a digital finance ecosystem, many users can simultaneously access the smart contracts. The processing of the requests for smart contracts is implemented in the cloud. Thus, the cloud platform needs a feature that automatically adapts its resources to the traffic workload level. It should allow the owner of a platform to run their smart contracts as microservices that dynamically auto-scale depending on various workloads. When the traffic workload is low, it should be able to allocate a few compute resources to save execution fees in the cloud. Also, it is required that when the workload increases, it should be able to provide additional machine resources assigned to the smart contracts until reaching the height of the workload level. Finally, when the workload increases further, the mechanism can use the appropriate scaling method, no matter through an increase in the number of computer resources on each VM or switching to another VM service category. All these ascending capacity methods should be transparent to the platform owner. This means that through the weight mechanism, the system should be able to implement the auto-scaling mechanism for adding newly highlighted cloud resources while serving orchestrations.

A smart contract on a PoS/public blockchain may be implemented as a microservice through a cloud platform. When users want to assign the smart contract orchestrations, the microservice needs to be located in the cloud. At the same time, it should be able to periodically query if orchestrations are being executed. If yes, it should be able to allocate/instantiate a set of cloud resources to the smart contract orchestrations to serve the transactions. When the transactions are needed to be sent on the blockchain, a particular microservice can be invoked to re-route those transactions to the respective blockchain. Given the assumption that a blockchain ecosystem requires a certain level of consensus in the aspect of ledger state, the realisation of cloud-hosted smart contracts is prone to trust issues. All new smart contracts need to be validated by the existing chain. Similarly, all transactions need validation before being locally executed.

4.3. Load Balancing Techniques

The concept of load balancing is fundamental to achieving high availability on any cloud infrastructure. For a host of processes running on VMs, load balancing is essential to ensure that all VMs are loaded uniformly and overloaded VMs are distributed appropriately so that no single node is overworked. In such a scenario, the ability to dynamically load balance massively parallel processes becomes crucial. Cloud infrastructure can be used to create an environment where VMs and processes can be dynamically created during load on servers or dropped in low load conditions. At the same time, wide area cloud infrastructures may also significantly reduce inter-cloud communication latencies, which requires dynamic processes and VMs to relocate to the closer server. Load balancing is the technique of distributing workload across multiple computing resources. Load balancing ensures no single load can be too much work for a resource so that each resource can function optimally while being reliable and available, among many other things.

Load balancing algorithms can be classified mainly on the following grounds as circular algorithm, random algorithm, minimum load algorithm, neighborhood algorithm, and weighted scheduling algorithm. In the circular load balancing algorithm, all servers in the network are arranged in a circular manner. Every incoming request is sent to the next server out of the server, the current server goes to the next server, and so on. The random load balancing algorithm selects a server randomly for service without any bias among the servers. The minimum load balancing algorithm checks for the load on the server where there is a minimum load among the servers. In the neighborhood load balancer method, each server actively does load balancing based on the load of servers in its neighborhood. In weighted scheduling, the load balancing is done based on the load of the heavy-weight process allocated to the server and processes with light workloads assigned to the servers in the neighborhood. Other main algorithms are round robin, least connections, IP hash, least response time, and load based scheduling.

V. SECURITY CONSIDERATIONS

Organizations (cloud service clients) should implement security control measures, enforce legal compliance regulations and conduct security audits; cloud service clients should request security audit reports as part of their pre-cloud

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91223

procurement decision. Organizations need to enforce legal compliance regulations to protect financial records, strategic plans, customer confidential information, and intellectual property. Access Control plays a pivotal role in governing how users with different roles will access cloud resources. The framework stores role-based access control policies in blockchain. Organizations and vendors run cloud resources locally, and they record cloud resource access logs in batches on blockchain. Smart contracts are utilized to limit the costs of this integration. There is a critical need to understand how the development of blockchain-based systems can align with the legal standards of an organization. Access Control investigates how cloud resources should be accessed. The framework adopts the role-based access control mechanism. Each cloud service client and vendor forms roles for their cloud resources. The roles along with role-based cloud access requests are saved within the blockchain. The blockchain stores hashes of policies as markers for the smart contracts, which hold functional codes that can be accessed by the public.

As mentioned earlier, organizations should trust the cloud service providers because they do not reveal information on a cloud platform. Nonetheless, trust is fundamental to financial organizations and enables a host of social and commercial benefits. Although organizations can implement robust access control mechanisms and encryption prevention to bolster privacy protection, access control breaches and data leaks are still widespread news. In the current cloud situation, organizations prioritize trusted cloud service providers. Trust is a pivotal construct for organizations since it is crucial for their reputation and public perception. A foundation of trust can only be achieved by establishing a secure flow of data transactions in the cloud environment. Digital Certificates create a chain of trust.

Fig 4: Data Security Consideration

5.1. Data Protection Mechanisms

The financing of small to medium banks was transformed by digital finance ecosystems. However, stakeholders in this space face zero-day exploits and could suffer significant losses because of financial fraud. In this environment, the emergence of cloud covering reservations is crucial. Additionally, this checks and maintains correctness and integrity. Furthermore, cloud resource capabilities can be leveraged for fraud detection and validation. Advaintedly, the ETL data preparation, knowledge graph construction, and batch inference of fraud check models can be performed on the cloud.

This approach is focused on building a solution called Grape. This proposes an architecture for scalable and secure digital finance ecosystems. Different potential mobile applications that help with the credit process of small and medium banks are targeted during the on-site app security evaluation. Installing vulnerable third-party libraries, leaking logs, and stale testing code were some of the findings. Initial direct code injection and a race condition each caused a leak of a user's private key from the Grape wallet. Potential mitigation strategies for the identified attacks are discussed as well, along with prevention methods and security best practices.

Data correctness and consistency are crucial to maintaining the system's trustworthiness. Ground truth and accumulated residual are the two states of the data. Unfortunately, smart contracts could be attacked. These include denial of service attacks through block gas limit, spamming, and data and time manipulation. Furthermore, due to an inherent limitation on the basic data structure of the chain, this might lead to a spam attack. The issue of off-chain credibility attacks is also addressed, which happens when on-chain events have nothing to do with the original smart contract. Besides misuse of funds, this causes a simple hack leading to incorrect information, resulting in incorrect credits. A data correctness

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91223

mechanism based on Merkle tree proof for better transaction security is proposed by maintaining the integrity and correctness of recording on-chain transactions and other data in the data lake architecture.

5.2. Compliance and Regulations

Adoption of cloud infrastructures brings additional complexity around compliance and regulations. Many novel-service architectures, especially multitenant platforms, mean service architectures may 'intrinsically' violate parental regulations. This is accentuated in large ecosystems with services from multiple first-tier service providers. Reasoning about compliance from regulations requires (i) obtaining and transforming compliance specifications into machine-readable formats and (ii) reasoning engines to check compliance. Using hybrid cloud infrastructures and ecosystems increases now the complexity of (i) and (ii). This leads to a need for a knowledge graph for compliance which can be generalized, enriched, and served by different compliance and regulator providers. Thus, a graph-to-graph transformation framework that would expose the internal structure of source knowledge graphs and would be used by reasoning engines to create different output formats. Ecosystems will be generically exposed in compliance knowledge graphs and will be functionally enriched and served by reasoning engines (whether internal or external). Finally, transformations from compliance specifications to compliance knowledge graphs need to be validated. Hierarchical domains where discovery relies on first-order logic induced hierarchies represented as bipartite graphs will be exploited.

Composite services with target invocation environments that are not benchmarked directly in the training of MAPE-P, will lead to noncompliance of regulations when invoked in such environments. This requires re-learning an IBN model for the new target invocation environment. Based on a subset of the variables of the source IBN model, the rewritten model is reusable, where each clause of this model strictly corresponds to a clause of the source IBN model, preserving its semantics. Service-oriented extensions are plan-based self-adaptive p2p systems where the plans control dynamically discovered peers. The peers can freely join or leave at runtime, which may invalidate the plan at runtime and threaten the compliance of such plans with rules. Knowledge graphs are exploited on a data privacy PDKI agent and supporting regulatory framework on an ecosystem-level graph.

5.3. Threats and Vulnerabilities

This section analyzes the greatest threats and vulnerabilities associated with FinTech systems and investigates their cybersecurity risks. Cloud computing's numerous cyber loopholes have increased awareness of security issues. Cloud service providers (CSPs) are often targeted by various forms of common threats that compromise computational and data resources, resulting in poor quality of service (QoS) or service disruptions. Cybercriminals frequently attack CSPs because they store vast amounts of valuable sensitive information. Since the abuse of FinTech privacy-sensitive data is an evolving and significant concern for organizations, state regulators, and end-users, attempts are being made to protect data from malicious acts. Previous studies have primarily examined general cloud security vulnerabilities that threaten the availability, integrity, and confidentiality of data and cloud-based applications.

Cloud service providers may find the cloud-computing paradigm attractive because it automatically accommodates the elevations in demand for performance and storage. However, this scalability advantage gives rise to unlimited access by equipment, software, virtualization, and storage vendors and resellers that sell or rent their services. Literature reviewed recent FinTech cyber incidents, categorized their causes, and identified their causes and consequences. However, regulatory frameworks that investigate and mitigate financial crimes do not consider the motives or tactics committed in which industry sectors. A publicly available comprehensive legal framework that discusses laws presented in legality, regulations, and policies concerning FinTech ecosystems and supporting technological infra-constructions is lacking. Misconfiguration of access control systems might have led to many dynamic threats from outsiders and insiders, imposing risks to privacy protections due to massive data sharing with third parties. Some data protection models have been presented to guarantee the privacy of customers' information.

VII. INTEGRATING CLOUD INFRASTRUCTURE IN FINANCE

Cloud computing has gained popularity in recent years for powering computing, storage, and networking resources for Internet businesses, and the financial sector is no exception. While leading global Internet or financial companies in China have begun to migrate their business to the cloud, cloud computing is still in its infancy in the traditional finance industry. There are significant concerns about the uncertainty of the future cloud business model, the security and compliance of finance data, personal private information leakage, and a lack of understanding of cloud computing in the Internet finance sector. The continuous emergence of industry-specific technology-driven platforms by fintech and cloud computing companies will pressure financial companies from both sides to reach a consensus and speed up the process of mutual standardization with open cooperation and the establishment of industry standards.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91223

Improve data credit investigation, traffic risk control, marketing strategy optimization, and customer management based on business transaction data and external data.

Moreover, cloud computing and big data are two disruptive technology trends. Regulating the digital finance industry amid the rapid innovation and implementation of these technologies is an unprecedented and ongoing challenge. A simple approach of extending existing regulatory policies to digital finance will not be effective due to the complexity of emerging business models and systemic importance. An analysis of new risks arising from the novel products and services of digital finance is conducted, highlighting four aspects of cloud computing data regulatory challenges and four dimensions of big data regulatory challenges. A regulatory approach that combines rule-based regulation, risk-based regulation, and regulatory sandboxes is recommended to facilitate the trading relationship between various stakeholders in order to promote a safe and inclusive digital finance ecosystem. The technical and economic mechanisms of regulating digital finance with the development of digital twin policy tools are discussed.

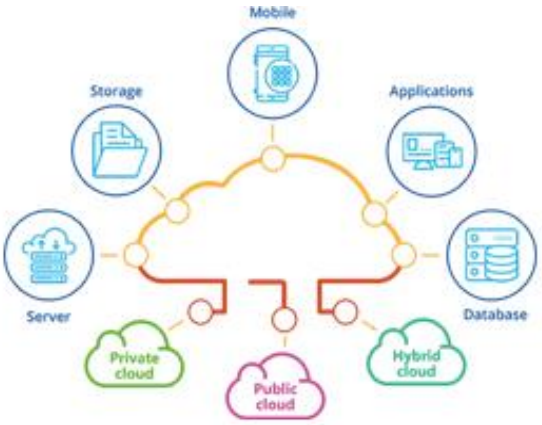

Fig 5: Cloud Infrastructure

6.1. Case Studies of Successful Integration

Based on the Report conducted by SIG Digital Finance Ecosystem, Cloud plays a critical role in building a Digital Finance Ecosystem. It helps 3rd party innovation, reduces the cost of participating in the Digital Finance Ecosystem, helps bring security and trust to the Digital Finance Ecosystem, and provides accurate data in a sound data ecosystem. It is a must for countries to develop Cloud Infrastructure. A central bank cloud helps more trust in the Digital Finance Ecosystem. A data clean room/sandbox cloud will help 3rd party firms in their innovation. In developing countries where data infrastructures are often lacking, designing a Cloud Infrastructure seems paramount and will benefit FinTechs as non-banking entities even more. As there is a vast lot of territory and population density in China, a chain-like cloud network infrastructure will help speed up the innovation and deployment of Digital Finance securely and beneficially. The Cloud will bring down Digital Finance costs while security remains a must. As data approaches better security through banks and trusted compute capability brought by the Cloud, trust will build up too. It needs to further educate the ecosystem stakeholders to understand the data's difficult nature, thus adopting proper data preparation, cleaning, and usage. Rules of the Data Ecosystem Design should be established and followed. The filter between the Data Ecosystem Builder and the Cloud Infrastructure Provider is healthy. Proper collaboration on the rules and data integrity will ensure trust in the data.

6.2. Best Practices for Implementation

The adoption of cloud-based infrastructure by financial institutions often leads to the creation of a multi-cloud construct. This construct consists of providers offering public and private services to a financial institution across different service domains such as SaaS, PaaS, IaaS, and DaaS. Financial institutions require a layer of control and visibility in such multi-cloud constructs to gain insights into the current state of their cloud assets, monitor systems and networks, and define policies that drive operational process integration. The technological evolution of the cloud landscape has led to a plethora of cloud providers across services, geographies, and deployment models, with the public cloud being the fastest-growing segment in the ecosystem. Institutions that share workloads across multiple clouds would need a multi-cloud strategy, with public clouds often being off-limits for sensitive workloads. Such a landscape of silos across geographies, deployment models, and service domains leads to high friction and complexity in ongoing management.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91223

The focus of any digital business strategy today is to provide customers with a seamless, enjoyable experience while maintaining the security and safety of their finances. These new operating models bring new partnerships, new services, and new delivery channels to interact with customers. The underlying technologies are the key to any future success in delivering this business transformation. Financial institutions want to take full advantage of the next generation of cloud computing to transform the way in which they develop and maintain software applications, customer experiences, and operational processes. This transformation can significantly reduce operational costs, provide the ability to quickly innovate with new services, and cater to increased demand at one time in high-volume environments.

Equ 3 : Security Posture Score

$$S_{sec} = f(E, A, C, D)$$

- E: Encryption strength
- A: Authentication robustness
- C: Compliance level (e.g., with PCI DSS, GDPR)
- D: Detection and response efficiency

VII. COST MANAGEMENT IN CLOUD SERVICES

As organizations migrate to the cloud, traditional forecasting processes may underestimate the expected cost and lead to situations in which the budget is exceeded. On the one hand, since public cloud platforms allow use-based billing, cloud resources that are unused can essentially be ended, leading to an increase of "pay-as-you-go" rates of tasks billed. Moreover, small test runs to evaluate cloud services are also charged even if they are only several hours long. On the other hand, cloud resources that are critically provisioned can incur on-demand rates leading to considerable over-budget. The flexibility and convenience of cloud infrastructures come with the drawback of unexpected cost surges.

For this problem, many budget solving methods have been proposed. Many methods rely on specific historical task and/or resource features to predict future consumption. These methods leverage the thresholded budgeting of resource over-utilization by controlling forecasted resource usage as bounded violation rates. Such budget capping methods lead to various overspending rates with different cost reduction guarantee levels. However, existing methods can lead to low budget prediction accuracy due to the high uncertainty in the cloud bank model. Moreover, budget predicting methods usually do not ameliorate the budget over-usage after its prediction.

Recently, methods that systematically analyze task history and compare the meta task performance with cloud competitors have been tried. This process allows users to better understand the available resources along with their pricing choices. However, such methods are usually resource agnostic which will lead to unthought through low performance choices. In addition, since public cloud databases keep changing rapidly, the need for using decisions might become obsolete over time. Such models relying on resource performance historical data and pre-optimizations hurt interpretability and consider task setup changes, etc.

In this paper, task-based budgeting prediction methods based solely on shopping prices and prior task load distribution of cloud infrastructures will be developed. The combination of task-based performance benchmarking and price-based resource selection according to budget goals will be also developed. Evaluation on cloud performance data and exploration of cloud use cases during competitions, hackathons, etc. has demonstrated that the proposed methods can predict budget goals with an accuracy over 80% across 7 datasets and select resource choices that provide advertised price advantages over premium cloud services. Cost saving of low-budget resources is also demonstrated by price-based selection.

There are multiple obstructions to using public cloud databases per se. Public cloud databases are themselves expensive and thwarted by a pay-as-you-go model which limits their offering and exploration. Similarly, query latency and cloud vendor lock-in can prevent the free usage of large datasets. However, cloud performance baselines are still promising, as only cloud performance data should be leveraged.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91223

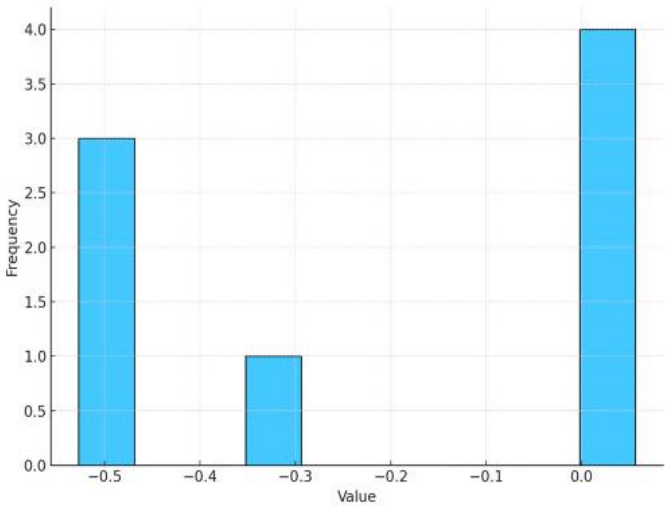

Fig 6: scalable and secure digital finance ecosystems

7.1. Understanding Pricing Models

The effective use of cloud computing technology has burst open new avenues of revenue and consumption. The cloud computing environment has offered a boon to the global economy. This paper focuses on the economics of the cloud environment. A comprehensive literature review identifies the cut-off points in the modeling of cloud environments. The focus of this paper is the economic modeling of cloud providers (CSPs) and cloud service users (CSUs). They offer and consume the cloud services, respectively. Each stakeholder has different economically valuable differentiating features on which various business models are founded. The paper details how modeling the economically relevant features of the stakeholders helps in studying the impacts of these features. It is summarised how the common building blocks of economic agents support the appropriate decision-making problems to be studied. The findings can assist researchers who wish to study cloud economic models and practitioners who wish to build sustainable business models in the cloud economy. In a right cloud ecosystem pricing scheme, new ecologies of businesses can evolve. The revenue generated will help customers invest more on new platforms and schemes. This can lead to a virtuous cycle between the cloud providers and customers. The transaction-based pricing scheme, which has the potential to yield variable pricing, offers this opportunity. Pricing innovations that can generate daunting amounts of data and user interactions can gain significant growth. The ability to analyze the data generated would provide a clear competitive edge.

7.2. Cost Optimization Strategies

Utilizing the native services provided by cloud vendors is another cost-saving method for cloud service consumers. Cloud providers offer many native, plug-and-play services that users can use to develop their applications. The nearly standard pricing of services also serves to boost competition between providers. To establish a data pipeline or application, there are managed services in each cloud offering. Managed services allow users to concentrate on the actual business problems and address them rather than spend time constructing the underlying framework. Managed services also offer a lot of built-in features, reducing the need for additional development and adjustments. Using native services can provide enterprises with many advantages. First, native services include optimizations that are invisible to users but enable lower-cost operation. Second, native services prioritize simplicity and guided use over attempting to expose the entire complexity. This does not imply a lack of adaptability; alternatively, they are the best way to access the capabilities.

Third, many high-level components and features for services are offered for free, but third parties will charge for them extensively. Cost-cutting for cloud services may have varying levels of abstractions because some providers also package features at higher logical levels (easy-to-use service levels). On the whole, numerous tactics can be utilized to optimize costs. Generally, cost optimization is interpreted as lowering costs while preserving agreed features and performance. Conversely, costs must be raised if it is evident from the outset that things will be better or faster. This has various interpretations vis-à-vis construction and workloads. For example, efficiency is key if a model or pipeline must execute thousands of times and results remain unchanged. This often involves tuning one provider or tenant and will frequently require significant adjustments to be transferable to others. Alternatively, if there are workloads incapable of flexibly scaling, the business has a bigger issue. Hence, cost optimization does not apply there.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91223

VIII. FUTURE OF DIGITAL FINANCE IN THE CLOUD

The future of digital finance will be reliant on cloud-based service models as organizations move towards digital transformation. As they embrace emerging trends such as product-as-a-service, platform-as-a-service, data-as-a-service, and brand-as-a-service, the finance industry must leverage cloud and AI. The tech and risk foundation needs to be restructured and, importantly, re-developed as dynamic, evolving ecosystems, where regulatory compliance, security, and privacy are intrinsically linked to the architecture, controls, and development processes. The conditions for success will include a new breed of analytics that is cross-functional, multi-domain, data- and AI-centric, and creates a unified view of the enterprise, customers, and risks to support innovation, and enable event-driven, and predictive decision making.

The cloud will provide an elastic, cost-effective, and scalable IT environment to run the financial ecosystem. The cloud model will be granular and multi-cloud in nature as networks of clouds will be used to run the different instances of the financial ecosystem. The cloud and AI models will be harmonized as the analytics will touch billions of data elements and images, and terabytes of data at the base level. A federated in-cloud execution of the different AI models will be supported by a continuous learning cycle to boost the performance and resilience of the financial services provided to customers by the ecosystem. These conditions for success will be further enhanced by building solid partnerships with technology vendors, regulatory bodies, and academic institutions. Strengthening the security/privacy risk framework that covers asset protection, threat detection/mitigation, cybersecurity resilience. The constantly evolving technology landscape will offer new opportunities/threats for finance, and the finance industry must adapt accordingly through effective risk and security management.

The finance industry will undergo a revolutionary phase in the next two decades. With the massive transformation of businesses, all industries must provide seamless customer experience, invest on maintaining a sustainable DNA in everything they do, and augment their capabilities to discover and respond to shifting business conditions with full visibility. This will be made possible by leveraging emerging technologies such as cloud, multifold AI, DLT, and quantum computers. The finance industry must strive to be ahead of the curve, riding the waves of the rapidly transforming technology landscape while carefully managing the threats that come with them since the challenges to comply with tightened regulations, and to manage mounting cyber risks would escalate exponentially.

8.1. Emerging Technologies

The emerging technologies are getting adopted massively world-wide in both the private and public sector. One of the well-known technological advancements is Cloud Computing. The number of Cloud Computing users is on the rise day by day. The adoption of Cloud Computing offers high-quality services at cheaper costs. However, this new paradigm has not been comprehensively explored by researchers. The main challenge to these emerging systems is the security issue. Security remains one of the bottleneck constraints in mass adoption of any technology, and so does the Cloud Computing paradigm. Cloud provider companies are doing their level best to provide secure solutions. This article will discuss how the cloud solutions work, the most critical defense pillars, and the ways to improve user experience. It will also explore the service and deployment models of Cloud Computing Technology and their importance.

Today, businesses are generating terabytes of data at large scales and sharing them with their clients and partners. However, the high cost of on-premise storage and maintenance limits the data storage and retrieval. Cloud Computing offers limitless opportunities in data storage and sharing. Cloud computing refers to a network of remote servers hosted on the internet to store, manage, and process data instead of the local server or a personal computer. Users can remotely access applications and services from any location through the internet. Similar to running programs in the machines of universities, governments, and other organizations, cloud computing works at the centers of web companies. Users do not need to install any software or configuration on their devices and simply access the services through a web browser globally. However, one of the main challenges today remains access control, which concerns the authorization or permission to the resources stored in a cloud computing platform. Many experts agree that cloud security is one of the open concerns of cloud computing innovations, and the industry is working to address this problem.

8.2. Predictions for Market Growth

Amid growing concerns about emerging risks and unresolved challenges due to accelerated digitalization and globalization, financial service providers are focusing on enhancing resilience and expanding the basket of solutions to customers with a renewed focus on sustainability. On these premises, the Global Financial Services Software Market is expected to grow exponentially during the forecast period, exhibiting a growth rate of 22.5% CAGR in anticipated revenue. With the increased adoption of AI/ML and cloud technologies, vast amounts of data are generated every day, creating new opportunities for innovation. Other market growth-driving factors include a heightened focus on customer-

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91223

centric insurance operations, live customer assistance with chatbots, and a surge in demand for data management, big data analytics, and business data warehousing solutions.

Despite the wide collaborative and regulatory initiatives undertaken for a better cloud asset security posture, the prolonged cloud asset management approaches, and the processed real-time data involved in manual attempts in today's digital world need to be further explored. Hence, a few opportunities are pointed in this proposed integrated framework that combines the unnatural and natural side of security in cloud resource management and need to be considered for security risk management. Firstly, various smart security approaches based on the current computing scenarios can be applied as a deployable component. Combining various models of smart security mechanisms by determining the failure rates and side effects of the security algorithms can enhance the integrity of cloud computing marketplaces. Cost-effective machine learning models can be utilized over complex decision trees due to the trained knowledge for runtime estimation efficiencies of new daily intake data. Streamlining technology devices in intelligent ways for solid real-time communications need to be explored further.

As large-scale storage ecosystems continue to proliferate, there is increasing concern over how to guarantee their efficient, robust, and cost-effective operation while ensuring data confidentiality and privacy for clients. To address this concern, this article proposes a scalable architecture for cloud object storage ecosystems. The architecture consists of a hierarchy of cloud servers connected by private leased lines, on top of which clients execute a multi-keyword query model that guarantees both privacy and efficiency. Each cloud server is capable of decrypting object (meta)-data while remaining oblivious to the contents of such data. To validate the efficiency of the proposed architecture and the multi-keyword query model, rigorous theoretical analyses and experimental results are provided.

IX. CONCLUSION

The accelerating presence of digital finance technology on the business scene in recent years highlights the evolution of a new digital finance ecosystem characterized by openness and dynamism. The development of digital finance does not merely guarantee new technologies or platforms, but rather necessitates the integration of local technologies and platforms into an organic whole that enables the co-evolution and synergistic effects of the entire digital finance ecosystem. From the perspectives of both the supply side and the demand side, the open co-evolution of the inducement, intermediacy, and switching costs ecosystem of digital finance improves the efficiency and inclusiveness of firm finance. The continuous co-evolution of this ecosystem is conducive to the governance of regular enterprises, counterfeit enterprises, and the ethical dilemmas of supplying data financial literacy. Academia, government departments, regulatory authorities, financial institutions, and enterprises expected to broaden the field of vision, concentrate on the layer-specific construction of the digital finance ecosystem, and initiate new dialogues and processes of co-evolution and co-governance.

Emerging issues of security by transparency and accountability in public cloud computing reinforce the requirement for manually recording all interactions, decisions, and transactions in the cloud to a local copy that can be audited later on by a third-party auditor which is tedious, time-consuming, and may lead to loss of information in case of auditor's negligence. Existence of a lot of vulnerabilities being caused due to a single point of failure makes it difficult to track user activities. Limited visibility of user permissions hampers the privacy of confidential data. However, with the proposed framework, these access control policies can be stored in an immutable ledger which ensures that logs remain unaltered and access management becomes easily auditable. In this work, an attempt has been made to tackle issues of unauthorized access and malicious activities leveraging smart contracts and encoding them with predefined rules. Their cryptographic underpinning ensures that even minimal tampering in the data can be easily identified. This automation in the process of data transfer between different parties in a secure way contributes to the resilience of the system and enhances user trust in the cloud. The challenges posed by the integration of blockchain with cloud computing, while enhancing security, may introduce network congestion and slower transaction processing speeds. There is an opportunity to resolve this issue by storing the fixed size of cryptographic hashes of the digital certificate on the blockchain linked with the off-chain repositories. The proposed blockchain-based architecture stands as a resilient solution and lays the groundwork for Trust Management in the public Cloud environment.

9.1. Future Trends

Cloud digital forensics is expected to undergo significant advancements within the next decade. Safeguarding the credibility and security of digital evidence in complex cloud infrastructures has become an active research and development focus as enterprises continue to adopt cloud services for data storage and processing. Proactive measures are needed to reduce the likelihood of incidents and to implement best practices for cloud service providers' and

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91223

customers' effective response. Particularly, the design of a systematic cyber-forensics readiness process is needed to facilitate the implementation of effective promoting measures. Numerous challenges and open issues remain in this domain. The complexity of cloud environments, multi-tenancy and virtualization, and data privacy and now sovereignty concerns compound the challenges of securely gathering and analyzing digital evidence. The evolving landscape presents exciting research avenues, as shared resources create new obstacles to forensic data collection and analysis further, and sophisticated cryptographic techniques aggravate the problem. Blockchain-based cloud systems add another challenge with decentralized data management and the validation of digital transactions. These issues continue to deserve full attention, along with delivering solutions to ensure the secure transmission and retention of data in and across diverse clouds while ensuring data consistency and integrity. The rapid growth of the cloud landscape is expected to generate challenges that require innovative solutions to effectively preserve and recover digital evidence, produce a secure chain of custody, and respond to the non-trivial issues resulting from clouds for data recovery.

On the other hand, expectations for the coming decade in cloud digital forensics focus on predicted developments in cloud computing and forensics technologies, some of which will have beneficial follow-on effects on legal, data, privacy, and sovereignty issues related to these areas. Key expectations include the advent of a storage-as-a-service system beyond anything known today; a one-to-many cloud forensic investigation model; the advancement of IoT for forensic data collection; faster cloud incident analyses and cloud digital evidence collections; and forensic investigation systems capable of analyzing data in mobile and fog computing environments. These forecasts are reflected in predicted cloud-related budget expenditures. The revenues of internet companies are expected to be substantial, with cloud services increasing their ratios by nearly half. With the increase in cloud storage, expectations for cloud digital forensics are that there will be a major surge in budget expenditures on cloud incident investigation and data retrieval technologies. Widely deployed and automated intelligent cloud digital forensics technology for prevention, detection, response, recovery, and follow-up auditing makes early detection of anomalies easier, they have not yet demonstrated means of surveillance without affecting privacy. Legal and compliance issues associated with investigations and regulations will be necessary for cloud digital forensics to remain lawful.

REFERENCES

[1] Karthik Chava, "Machine Learning in Modern Healthcare: Leveraging Big Data for Early Disease Detection and Patient Monitoring", International Journal of Science and Research (IJSR), Volume 9 Issue 12, December 2020, pp. 1899-1910, https://www.ijsr.net/getabstract.php?paperid=SR201212164722, DOI: https://www.doi.org/10.21275/SR201212164722

[2] Data Engineering Architectures for Real-Time Quality Monitoring in Paint Production Lines. (2020). International Journal of Engineering and Computer Science, 9(12), 25289-25303. https://doi.org/10.18535/ijecs.v9i12.4587

[3] Vamsee Pamisetty. (2020). Optimizing Tax Compliance and Fraud Prevention through Intelligent Systems: The Role of Technology in Public Finance Innovation. International Journal on Recent and Innovation Trends in Computing and Communication, 8(12), 111–127. Retrieved from https://ijritcc.org/index.php/ijritcc/article/view/11582

[4] Mandala, V. (2019). Integrating AWS IoT and Kafka for Real-Time Engine Failure Prediction in Commercial Vehicles Using Machine Learning Techniques. International Journal of Science and Research (IJSR), 8(12), 2046-2050.

[5] Ghahramani, M., Qiao, Y., Zhou, M., O'Hagan, A., & Sweeney, J. (2020). AI-based modeling and data-driven evaluation for smart manufacturing processes. IEEE/CAA Journal of Automatica Sinica, 7(4), 1026–1037. https://doi.org/10.1109/JAS.2020.1003114