Deep Science Publishing
https://doi.org/10.70593/978-93-49910-98-0_5

Chapter 5: Establishing secure financial infrastructure using cloud computing and encrypted data management

5.1. Introduction

A cloud computing offers numerous advantages in terms of cost strictly compared to the other models, i.e., it makes available to a broad audience the opportunity of taking advantage from provided infrastructure and services. However, it introduces new security and reliability concerns. Financial Institutions had to spend a lot of efforts in keeping data safe and protected. These sensitive data – if affected by breach – are able to damage customers to the same level of institution, with a risk for consumers of loss or damaging of capital and for banks or financial institutions of losing market share, damage to brand or revealing of confidential information (Zhang & Liu, 2022; Desai, 2024; Lefevre, 2024).

Hence, for financial area, it is mandatory to build a secure ecosystem and keep only some limited parts in cloud. It is also important to focus on monetary transactions that due to a high volume can become profitable in order to implement a process for managing risk and security for those transactions. Moreover, it is relevant to manage the stop moment – the moment before the transaction that can be interrupted if detected as not credible – and this should be in pure low latency since money travels with high speed and at low cost. Protecting institutional integrity and availability of data becomes critical and sensitive at the same level of confidentiality. The final goal is to build a life cycle for institutional data that does not introduce flaws with damage limits (Alexander, 2025; Roy et al., 2025).

5.2. Overview of Financial Infrastructure

Various types of networks such as roads, railroads, coaxes, wires, electric power lines, drinking water pipes, water disposal pipes, and so on are commonly installed and connected with each other, creating a cooperative and comfortable living environment.

Therefore, these original networks are called infrastructures. Financial incomes and expenditures of each individual and organization are complicatedly connected with each other to create a foundation. This is the basis for economies, at a national level and on a global scale, to operate. Therefore, the financial income and expenditure infrastructure is overlooked, but upon removal, the ecosystem collapses. And any nation needs such an infrastructure to safely operate the economy. In that sense, the financial infrastructure is vital to any nation.

Security infrastructure, via cryptography, provides a protective shield. However, if security is required in a transaction or operation which holds a huge number of participants, using these encrypted data may bring serious overhead. To eliminate such heavy burdens, some consensus procedures are currently used. Blocktechnology is one of them, and is now expected to create a new distributed collaborative environment in cyberspace. The paper introduces some traditional financial and security infrastructures finally resting on the centralized approach as a basis, and then discusses cloud and blocktechnology based new infrastructures.

5.3. The Role of Cloud Computing in Finance

Cloud computing is quickly becoming a standard element in many elements of business provision, not least the financial sector. Cloud financial services include payment processing management exclusively designed for fintech companies, deploying enterprise-level solutions, providing internal database for private equity, hedge funds, and investment banks, providing integrated solutions to financial business in the areas of payroll software and offering wireless solutions for terminal and web-based merchant services. This is to be an attractive bundle of services, especially the reduction in processing costs since with lower overhead costs the providers of the cloud services can pass on lower tax to the clients.

Cloud computing enables much more cost-effective and faster deployment for financial houses through its three major characteristics, i.e. multi-tenancy, on-demand service, and pay-as-you-grow model. The challenges and risks associated with cloud financial services are, however, non-trivial. With sensitive data at stake and heavy regulatory restrictions related to data residency and consent, banks or financial institutions risk liability for violations of these requirements when they outsource their operations to a cloud service provider. In addition, sensitive and highly confidential financial information which banks keep concerning their customers including account balances, transactions, and consumer credit histories are at high risk from privacy and security breaches when these data travel outside or on the Internet through the cloud and are kept on computers and data storage systems in foreign countries. Generally, there are two main categories of security threats to the data hosted in the cloud. The first is the

unauthorized access to the cloud data from outside the organization. The second is the compromise of the trusted insider account used to gain access to the cloud data. Safe processing of data in the cloud, encryption of data before upload, and encryption of keys to encrypt data are some of the commonly used techniques to secure data in the cloud.

Fig 1 : The Role of Cloud Computing in Finance

5.3.1. Advantages of Cloud Computing

Cloud computing is normally defined as the product of the achievement of distributed computing that enables clients to consume dynamically and on-demand network accesses of shared configurable computing resources. Cloud computing is promising to grow as a revolutionary model of shared computing platforms that can make services available in a more efficient, scalable, and sturdy manner. Unlike the previous distributed computing model where people need to invest heavily to establish their own grid and allocate sophisticated IT people to build and program their applications, with the new

cloud computing model, people can simply build their application services on top of the computer services provided by cloud service providers and just pay for the consumed resources.

The main advantage is that it eliminates the need for banks to make huge investments in establishing and operating big data management, data security and risk management infrastructures, which normally require heavy investment from banks with highly sophisticated IT teams plus years for systems development and testing and also constant running costs. In addition, by using a shared cloud computing infrastructure, banks' customer service infrastructures become more scalable and more flexible because if banks want to expand their existing applications services, they can simply request the cloud providers to give them more resources using the pay-as-you-grow principle.

5.3.2. Challenges and Risks

There are several factors to be considered while moving the financial infrastructure to the cloud. One of the factors is security. Traditionally, financial institutions are used to silo their data and infrastructure in on-premise solutions. Possibly the biggest concern, and the one leveraged by those who propose "building your own" solutions, is security, especially privacy. Among their tasks, banks have the responsibility of ensuring that sensitive customer data is not stored anywhere except in security hardened location. Nowadays, hackers are developing more sophisticated attacks and techniques in order to steal credentials, passwords, personal financial information, and social security numbers. There are threats to the financial industry, including hacking, malwares, and phishing attempts.

These threats have all systems vulnerable to be accessed. So the question is still open if a private cloud or an on-the-premises model can deliver better security than a public cloud model. Security breaches have happened to both models, proving that security safeguards need to be in place in all solutions. Though cloud providers have very sophisticated mechanisms put in place to ensure protection of sensitive information, in effect shifting the security concern from the enterprise to the cloud provider, it is still the responsibility of the enterprise to ensure the cloud provider is capable of dealing with the scale of those threats. Security, privacy, and regulatory compliance need to be carefully considered, otherwise they can become blockers for company cloud deployments or also for entire industry transitions. Sensitive data like customer information, financial transactions, or security positions must be protected, both at rest and in-flight. Innovations in encryption techniques can enable data holders to successfully move some or all sensitive data to the cloud, while still enforcing policy compliance and risk mitigation.

5.4. Data Management in Financial Systems

The cost of service provision is one of the most important factors in financial activities; therefore, all financial institutions strive to optimize the costs of providing services to customers. One of the most effective technologies for cost reduction is the automation of processes. To do this, companies use various software applications that centralize the data used in these business processes and ensure the end-to-end history of changes made to them. From the business point of view, the described process consists of creating electronic documents that represent financial operations between the subjects involved in the service process, including funds. Preparation of financial documents is the basis for creating and maintaining the data model of the financial institution. The implementation of such a solution doesn't mean at all the complete satisfaction of the customers. If the financial company uses a model of asset-backed financing, then with existing costs for good clients, the rest will need to pay more. Establishing a secure data management environment will help banks attract customers with better conditions.

Data management is a set of managerial decisions and actions that ensure planning, organization, technology selection, implementation, and resource management during the data lifecycle. To create a long-term capital acceptable to the risk profile of the financiers of the financial institution and, in particular, the clients of a bank or bank holding company, the bank should create all the conditions for conducting an efficient banking business. Indeed, the concept of information lifecycle management initially described a way to manage multiple data types to minimize cost and risk at each business life cycle stage. Since company data can have different importance levels and characteristics, data management defines different approaches to data class management.

5.4.1. Importance of Data Management

Management of data comes in many forms, both technical and organizational. All known bank transactions eventually generate data. A bank accounts manages customer's data including identification, verification, responsibilities, and transaction history. A customer or supplier master data includes technical identifications for inter-company data exchange, payment instructions including bank accounts, and addresses. Associated with all of these data is meta-data describing its structure and contents. Bank data policies set out rules and constraints for data management. Data in a computer system exists for access, sharing, and use in many diverse and independent business processes. Business flow systems lead to permanent transactions say in a bank central system. Data, and the ability to access it in a timely and trustworthy manner, are essential to success in any effective business. Traditional sources of competitive advantage are being replaced by the ability to manage access to data more effectively than one's competitors. Traditional transaction flows, from customer to accounts receivable, to cash collection

and accounts reconciliation, are now being replaced by bank negative cash flow models that depend on access to accurate and up-to-date financial and accounting data.

Data management is a key function both at a bank and by a bank. Banks have been asset and accounts custodians for many centuries, usually in paper form. In order to move to the new challenge carrying out virtual bank transactions based on electronic rather than paper access, banks have to renew their focus on customer data management variables of organization, people, and technology. The large increase in bank customer transactions has resulted in a significant expansion of bank operations. Modern computer systems as well as data handling processes are well suited to handle this increased volume of transactions. Bank data management systems answer the challenge of customer data storage, retrieval, and transaction processing.

5.4.2. Data Lifecycle Management

Data lifecycle management (DLM) is defined as a dynamic and complex discipline with the aim of fulfilling the data systems requirements and user security policies, such as security, accessibility, confidentiality, and integrity. DLM operations and activities accompany the data during its lifecycle, which extends throughout creation, storage, sharing, processing, performing transactions, deletion, certification, and archiving. DLM aims to facilitate the management of Financial Technology infrastructures by introducing privacy and cybersecurity in each of the phases the data goes through. A specific data lifecycle is modeled, and a related policy is designed by security officers in compliance with financial regulation. This policy presents the requirements imposed on data at rest, in use, and in transit, which are the main pillars of the DLM. The proposed approach introduces an architecture that automates the specific operations that implement the DLM policy. Through such automation, the management of information and the levels of cybersecurity and privacy may be improved while guaranteeing user productivity. Specifically, the architecture provides a tool that reduces the complexity of the different technological solutions that guarantee privacy and cybersecurity without hindering user activities. DLM for fintech infrastructures is a fundamental aspect to keep in mind as it is central to the model proposed. The interest in privacy and cybersecurity is intertwined with the interest in infrastructural performance in terms of scalability and cost. Data lifecycle management could impact the scalability of the infrastructure due to the duplicated data necessary to store encrypted information on the cloud while making it accessible in the various operations the data is subjected to during its lifecycle.

5.5. Encryption Techniques for Data Security

The key attribute that guarantees confidentiality and security of the medical records is encrypted data. Encryption converts plain text into cipher text by using cryptographic algorithms and encryption keys. Any sensitive data, after encryption can be transmitted through channels and stored on disks confidently. Encryption is a method of protecting data. This process transforms the data, making it unreadable to anyone without a decryption key. Encryption cannot protect data completely, but it is considered the best way to securely store data. Encryption has been available for thousands of years. However, the development of computers would bring new, more sophisticated processes and security methods to encryption. There are two groups of encryption algorithms, symmetric encryption and asymmetric encryption. Symmetric encryption is the standard method that uses the same key to encrypt and decrypt the data. It is faster and easier to use than asymmetric encryption. However, the need to share and then protect the keys introduces a serious security risk when using symmetric encryption methods. Because of its speed and strong level of protection, symmetric key encryption is best suited for protecting large volumes of data. Usually, symmetric key encryption is limited to applications involving one person and one trusted server.

Asymmetric encryption, also called public key encryption, uses two keys instead of one. One key is known by everyone and is used for encrypting messages. The second key is known by the intended recipient and is used for decrypting the messages. Because so few transactions use asymmetric key encryption, and because of the additional overhead involved with asymmetric encryption, these systems do not require the speed of symmetric encryption systems. As a result, asymmetric encryption is adopted for data transmission. Usually, asymmetric encryption is applied together with symmetric encryption.

5.5.1. Symmetric vs Asymmetric Encryption

Cloud computing is untrusted since cyber security is difficult to maintain. The massive data storage and management of sensitive data in cloud computing make symmetric and asymmetric encryption for securing these data important. Data encryption helps preserve the confidentiality and integrity of sensitive data. Once the information is encrypted properly, it is incomprehensible and unreadable until it is decrypted with a specific key. There are two main kinds of encryption: symmetric and asymmetric. Symmetric encryption uses a single key to encrypt and decrypt the data. The same key must be shared between the participants to ensure that the encrypted data can be decrypted properly. Asymmetric encryption works using a pair of keys known as public key and private key, which are mathematically related. The public key is used to encrypt the data while the other private key is specifically used to decrypt the data. The private key is not

shared, while the public key is available to anyone detectable by the participant who possesses the private key.

Symmetric encryption is much faster than asymmetric encryption. In symmetric encryption, the data is encrypted and decrypted using the same key, as a result, symmetric is also referred to as conventional or secret key encryption. The key must be shared and kept secret between both participants to ensure that the encrypted data can be decrypted properly. Symmetric encryption has several drawbacks. The fundamental issue with symmetric encryption is the increased complexity of ensuring that different keys are used for different communication sessions and at the same time protecting the keys from discovery. Each pair of users must share a separate key. For different users, a number of keys need to be shared which is impractical. Also, key management becomes difficult when the participants are not decided ahead of time. Even though symmetric encryption is fast, it cannot be used to encrypt every available piece of information because of its overhead of key management and distribution and, because there are many more operations available for asymmetric than for symmetric encryption.

Fig 2 : Symmetric vs Asymmetric Encryption

5.5.2. Encryption Protocols

The problem is then how to implement the symmetric encryption systems most efficiently. In particular, for a reasonable level of security, the most efficient symmetric

encryption system is the well-known Data Encryption Standard. In this standard formulation the key is K = Ks.

To reduce the size of the key, the standard uses a 56-bit key that is systemically expanded to generate the large-size key variant. Next, in the most well-known protocol, the maximum block size is equal to the data word size or less and equal to 56 bits. Such small block sizes guarantee a reasonable speed of encryption. However, earlier DES-based protocols cannot guarantee an appropriate level of security because of the small-size key K. To address these new threats posed to symmetric encryption protocols, the new AES algorithm was also proposed. As compared to the DES system, the new AES standard proposes more secure key variants and more secure message block sizes.

However, a number of observations can be made about the two systems. First, the public-do-not-have-keys systems provide no protection for the general public when asymmetric-key encryption is used. On the other hand, the asymmetric protocol does not seem to be the most efficient system, either because of speed limitations or a lack of data-size capacity because of too-small data processing block sizes. Secondly, high-performance network servers and clients always have similar pairs of private/public keys associated with the authentication-factor e and forgettable user password w or the authentication-factor d. The e and d keys have to be sufficiently complex to provide an appropriate level of security. Finally, when large data are involved, efficient protocols related to the public key cryptographic system cannot be used.

5.6. Integrating Cloud Solutions with Financial Services

Cloud computing undoubtedly makes managing financial operations far more manageable both for financial institutions as well as for third-party institutions. Cloud computing has developed and modified the Company's financial business attitude by creating new, dependable, and affordable applications. The financial company was previously apprehensive about providing data to third-party vendors and did not want to risk sensitizing, protecting, and monitoring deeds. Data privacy was a major hurdle, but the new compliant, secure cloud set-up for sensitive information storage has audibly modified this attitude. Most organizations currently have some form of cloud strategy in place. In the next several years, we should expect to see an accelerated transition to cloud solutions for IT applications inside the Financial Services sector. Nevertheless, Financial Institutions still need to solve several issues related to technology management, things like company compliance, security, regulatory obligations, transfer of information and technology.

The cloud provides a sufficiently reliable solution for a variety of areas and functions in the financial institution. Cloud computing can improve the beta where hedge-funds

execute testing models by transferring deeper search knowledge. For businesses, this can trigger more structure and probably even more results from programs. In Portfolio Management, Cloud computing can enhance the portfolio optimization and execution situations in the financial company. Portfolio help can readily take place in a cloud environment with Tech solution providers taking time and cost design concerns into orientation. Security Analysis, a focus area for most Financial Firms in today's World can buy cloud-computing. Reducing costs by taking risk reducing approaches in a cloud environment focused only on security and related probabilities for customers and Finance businesses can offer Mutual funds tech costs which are insufficient currently.

5.6.1. Choosing the Right Cloud Provider

A primary goal of cloud security is to provide a similar level of security to that which would have been provided by an on-premises solution. Before selecting the cloud strategy or provider for their operations, CISOs should make a security-related checklist and confirm the proposed provider can provide the security definitions in the signed agreement. The cloud provider should provide security. But it should be supported by trust in the cloud services. Nevertheless, applications and user access still need additional controls provided by the organization to ensure adherence to corporate policy and regulatory requirements, especially as they relate to data security, information security, and identity management for sensitive databases.

Typically, a cloud service provider is responsible for the security of the services provided and the customer is responsible for securing the information and data within the service. The shared responsibility model for security requires that both the provider and the customer take responsibility for building the right security model around the specific services being considered for deployment. Shared responsibility models for the security, compliance, and regulatory activities for the major providers show that the definition of security requirements and appropriate data protection is a primary responsibility for the customer. It becomes increasingly critical for customers to work closely with providers to understand the deltas in security solutions.

As part of the requirements definition, it is imperative to assess the certifications associated with your decision-maker. Cloud security looks different for different providers, so make sure you conduct due diligence and research the security offerings provided by your top cloud service provider candidates. Costs will vary. Make sure the options that matter the most to you do not require paying for superior service levels you do not need for your applications.

5.6.2. Compliance and Regulatory Considerations

The financial services and technology business is actually one of the most highly regulated sectors in the economy. For those who either provide financial services or businesses whereby the customer provides their financial data in any form, it is critical to understand this landscape and abide by it. Failing to do so can create major problems, opportunities for litigation or fines, or can severely damage the trust relationship between a customer and the business. Whether it is that regulates your business, specific requirements must be adhered to, including risk assessments, privacy policies, continual auditing, data security, secured file storage, and data access restrictions.

Not all cloud providers are created equal in the eyes of the regulators. Aspects that are considered are the physical locations of the datacenters, policies governing the access to the data, secure communications, and immutable logging of all administrative activities around the data. The provider should also have the appropriate certifications and there should be regular audits conducted by either internal auditors or independent external auditors. Additionally, there must be well-documented Business Continuity Plans along with Disaster Recovery Plans. These designs must be continually exercised and tested to ensure that the proper response will occur in case of a major incident. Failure to comply with these mandates can quickly be discovered during a regulatory audit and can have serious repercussions.

5.7. Case Studies of Successful Implementations

Despite the numerous advantages of traditional hosting, the financial services industry remains convinced of the security, compliance, and reliability of on-premises data centers. At the same time, the latest technology provides numerous capabilities that allow financial services institutions to maximize their profits while minimizing their efforts to ensure secure and rapid transactions. As a result, the financial cloud model is appearing, in which banks and financial organizations share a common cloud infrastructure that is designed specifically to address the security and regulatory concerns of the financial services sector. The financial cloud sharing model relies on state-of-the-art cryptographic techniques, regulatory compliance and governance, and mature infrastructure and operational processes. This implementation has enabled various sectors of financial services infrastructures to gather more information faster, allowing insurers to handle risk and enhance business results. These case studies demonstrate different challenges financial institutions face in using the cloud and are examples of how they overcame them.

In July 2020, one of the largest banks in the United States made the news after a successful implementation of a cloud platform to strengthen data-driven innovation

efforts and offer more financial solutions to clients. However, many banking industry executives were concerned about this implementation due to the high level of protection against data loss possible by only an in-house data center. In fact, many financial institutions have come to rely on the cloud infrastructure for multiple services, such as risk analytics, surveillance, payments, wealth management, market analytics, and critical operations, especially during the pandemic that required physical distance to prevent the spread of the disease. The latest cyberattacks against big banks, however, led them to again implement zero-trust and multi-factor authentication for all users in different roles aiming to avoid unauthorized access.

5.7.1. Banking Sector Examples

International data reveal that a considerable portion of banking processes and procedures has already been computerized, which means that much of the data flow and data maintenance can be done via the Internet. Encryption applied to very sensitive client data may advise that this data should be kept in-house and not in the cloud. Banks are thinking about working with mixed cloud systems, private clouds with selected strategic suppliers. However, some of them are already working with complete solutions, based on the cloud, as a case of production both clouds for production and a whole offer of services in model.

A bank based in Spain has penetrated the cloud offered by a major provider and is already implementing it. The platform has allowed the bank to improve its digital services, making transactions more dynamic, particularly in the mobile phone segment. Cloud computing offer from large technology companies has gained strength in banks. Several of them are noticing the announcement of expansion investments in this area. Economic recovery looks ahead for banks and increasing their stock market value. The aim, in addition to reducing operational costs, which may reach levels close to expenditures, is to increase the control of critical business areas, in this case, consumer loans. A banker aims at restoring cloud strategy after a period of suspension of its investment strategy in technology. The strategy of a major bank, which has sheltered in several industries, wants to further explore investments via a hybrid model as a way to ensure the security of its businesses, and to create a single central location for the integration of data analytics and cloud computing.

5.7.2. Investment Firms' Strategies

Goldman Sachs was one of the first major firms on Wall Street to invest in cloud computing. Back in March 2017, Goldman letting an insider know that they expect to rivet on developing their cloud-based data-sharing system that would make it easier for

different divisions to chunk box data and all build their own technology on top of the structured information. Goldman Sachs cannot compete with major Technology firms, and borrows the services of some of them, but Goldman is the main executor of the strategy. The tech giants are the service partners here. The firm continues to undergo a full-fledged digital transformation, specifically by creating a sleek new platform for credit cards and payments that it hopes will chisel out a thicker wedge from the lucrative financial technology market, which has been deemed approachable only for exclusively tech or fintech firms. J.P. Morgan has also full-fledged absence in cloud strategy. It inked a deal to use its cloud platform, while also building its own services and those for clients, including products that conserve existing onsite systems, and products and services for customers on the cloud. J.P. Morgan has also used multiple cloud platforms, which indicates multiple clouds are in the strategic strategies of investment management firms. Experian, who market data for asset managers, investment banks, hedge funds and pension funds, has done a one-off deal with a cloud platform. The company has heavily invested in cloud infrastructure over the last few years, with plans to build on their deal with cloud partners to streamline secure client onboarding and enable fund managers to incorporate experience and regulatory involvement into their strategy decision engines simply and conveniently.

5.8. Future Trends in Financial Infrastructure

The sustainability and growth of the global economy relies on continuously developing merchant payment processing technologies. Organizations that do not embrace these changes risk falling behind and eventually failing. The development of technologies like artificial intelligence can help in avoiding fraud and the onboarding of the lenders will be completed through automated processes. However, the use of neural networks will require long-term data that will enable the networks to learn patterns and detect violations. These fields are not yet widely used, and the knowledge required for developing neural networks or training them on time series data is rare. However, soon as these processes are developed and become easier to engineer, it is likely that they will significantly reduce risk and allow lenders to serve markets that have become unattractive due to large risks. Other technologies that can potentially offer significant enhancements to payment systems are blockchain technologies. They can easily provide a bridge between central banks and crypto payment platforms, greatly improving and reducing the costs of using such services. In general, developments in the cryptocurrency world seem to seek a bridge to traditional finance, rather than undermining it. Banks offer digital wallets while fund management companies evolve into exchanges through their capacity to offer the management of crypto funds and protect the assets. Institutional investors demand custodianship from large banks to invest in cryptocurrencies. There is a strong indication that government intervention could

interfere into the degree of establishment of cryptocurrencies and CBDCs. A frictionless digital economy should allow us to purchase goods in either fiat or cryptocurrencies, paying via either of these two methods, or by using a combination of these means. In general, it is likely that in the future, more financial services will be provided through the cloud. Demand for SaaS solutions has been growing during the crisis and with the inevitable growth in the adoption of these methods, we can also forecast a reduction in the research and delivery costs associated with these solutions. This should in turn decrease the number of banks that choose to invest in the infrastructure to offer banking services through on-premise solutions. However, the solution might also be demand-driven. The presence of larger systemic threats such as cyberattacks or pandemics could lead several countries to consider securing their national financial infrastructures, leaving no banks to be connected to the systems through the cloud. A balance in the demand for cloud services will be reached.

5.8.1. Emerging Technologies

Emerging technologies such as Artificial Intelligence (AI), Blockchain, Quantum Computing, edge computing, and the Internet of Things (IoT) are already influencing clouds, the connected devices that access cloud services, and the applications implemented in the cloud. AI-based services are already widely provided via the cloud. As cloud providers continue to implement the latest algorithms and ramp up their infrastructure to support them, use of AI as a service will continue to grow. These companies afford advanced analytics, machine learning, and AI capabilities. The emergence of AI will not only enhance existing cloud services but also accelerate implementations of augmented business applications.

Whether decentralized or federated, Blockchain technology has the potential to change the way the identity of people is stored and managed, the way data is secured and shared, the way trust within business and financial ecosystems is formed, or the way the economy and the business ecosystem are modeled. Due to the distributed and immutable nature of Blockchain-based architectures, users can own their identity and transfer it securely without going through centralized identity providers. As a result, Blockchain technology increases privacy design capabilities for applications without losing trust, accountability, and data integrity. By supporting decentralized identity, Blockchain-enabled clouds can provide integrated services capable of authenticating individuals without third parties, thus allowing the automatic running of directives of identity owners.

5.8.2. Predictions for Cloud Adoption

When exploring predictions for cloud adoption, it is important to clarify for whom we are making predictions. Different users have different needs and vendors support those differences in different ways. We will try, in our prediction, to encompass likely adoption patterns for the main groups of stakeholders. More specifically:

- Software as a Service Vendors and their Customers

- Platform as a Service Vendors and their Customers

- IT Departments

- Line-of-Business Customers

- Application Development Departments.

A prediction for all of Application Development is likely to be short-sighted and politically incorrect. For example, a section could easily conclude that the size of the business will grow in parallel with the size of another business. But this begs the question of which service will grow faster and why. A possible conclusion could be that the role of the user and the context determines how much and for what the user will rely on third-party technology providers.

An alternative to such predictions is the concept of broadening the adoption to support internal data sharing where IT management in large enterprise would provide a background collaborative data-sharing infrastructure that can be used by line-of-business customers. Assuming that would indeed promote internal sharing, the external might end up hurt since the IT organizations that enable internal places might well choose to rely on composite solutions, data on-demand, mini-solutions or even picking existing applications and recreating them internally. But these rival application development choices remain detached from the cloud computing discussion, especially if you believe that cloud computing is essentially another mode of outsourcing application development.

5.9. Risk Management in Cloud-Based Financial Systems

In this section, we provide a comprehensive overview of how risk is to be assessed, mitigated, and managed, thereby offering a “how to” methodology to the practitioner on how to perform risk assessment and mitigation. The basic principle in any cloud-based financial service, from the transfer of data to the enabling and transfer of money, is the storage of sensitive data outside of the security perimeter of the financial entity offering the service and therefore handing over the security control of that data to a third-party

cloud provider. This trust model creates a vacuum in which the enterprise loses its barriers to data security and becomes entirely dependent on the cloud provider to provide the controls which would normally be in place were that data still within the enterprise perimeter. Data loss, plaintext loss, unauthorized access, exposure or sharing, insider threat, data corruption or modification, service inconvenience, loss of control, tenant isolation failure, compliance-related events, denial of service, and data processing violations are the multitude of concerns facing entities using the cloud to provide financial and commercial systems and services.

The growing reliance on cloud-based financial systems requires organizations to proactively identify and mitigate risk. Many financial institutions require high security and data loss prevention, as it is critical to their business and business operations. Financial institutions provide cloud service with encryption for data protection and risk management of service offered to their customers. Our model provides a scope for account compromise prevention, data loss prevention, data retention, and key protection. Using the data security measures defined in our model will ensure better security, dependability, availability, and processing control for the financial sector. Financial institutions can adopt general risk management policies or industry-specific measures to protect their assets and customers. Indicators for cloud service consideration should include criteria such as risk levels, exceptional financial transactions, the level of consumer education and awareness, customer assets relative to the deposits from the merchant, identify technology capabilities and the strategic system.

5.9.1. Identifying Potential Threats

The success of cloud financial infrastructure hinges on the management of identifiable risks. Such a success is further realized when these potential risks are well articulated. Risk mitigation strategies can only be designed after identifying the core risks and threats. Risk identification is an ongoing process that needs to be performed on volatility intensive environments like banks. Disturbance theory is useful for understanding the timeline of possible events that could have consequences. There are lessons learned in disturbance theory that could help cloud service brokers realize possible threats. For financial institutions the biggest risk is being liable for illegally around unauthorized money transactions. Because cloud service brokers are the main components of the cloud infrastructure, they are responsible for the security of the cloud infrastructure. Banks internal deployment strategy becomes only important for organizations that deploy the bulk of their applications internally. However, most organizations will still depend on the CSPs for services they no longer wish to manage internally. It is also a proven fact that problems such as disclosed information, data destruction, and at worst cases a complete data theft, happen through CSPs; hence, they are key entities in the cloud

infrastructure that need risk management. Information systems outsourcing claims benefits for organizations; however, for banks and financial organizations interconnected through the financial systems, the costs imposed due to mismanagement of risk are high. With the movement towards self-regulation, the current structure requires that organizational risks related to illegal money laundering amounts to sizeable fines imposed on individual organizations.

5.9.2. Mitigation Strategies

Mitigation strategies detail the different layers of security to protect data from being compromised. There are three strategies to protect sensitive data in the Cloud, these are: removing sensitive data from Cloud, protecting sensitive data, and controlling access to sensitive data.

The simplest way to secure sensitive data is to avoid processing it within the Cloud. For example, using authenticated encryption reduces the sensitive data that need to be shared with the Cloud, in transactions where transfers of encrypted data should happen. Part of the sensitive data should stay out of the Cloud. While Cloud accelerates many transactional processes, there is no obstacle that prevents centralized transactional processes from operating privately on Local Area Networks or Wide Area Networks controlled by companies involved in the transactions. The strategy of not using Cloud resources for sensitive transactions could then preserve individual privacy and significantly increase the difficulty to hack sensitive data during transit.

Another strategy is to encrypt the sensitive plaintext data that will be temporarily placed in Cloud servers and whose security need only last for the duration of the Cloud server operations. The Cryptographic Correlator allows server-side computations on data encrypted without being decrypted. The correlation appears to be done on the plaintext, but it is done in the ciphertext. Only the final restoring step applied after these computations decrypts the final result and is not reversible by the Cloud infrastructure. Encrypting sensitive data with the Cryptographic Correlator and letting the Cloud infrastructure execute operations on the encrypted data allows keeping sensitive data encrypted up to the last possible point, potentially offering storage and communication temporarily protected to the Cloud provider without custodial or administrative access to sensitive plaintext.

5.10. Best Practices for Secure Data Management

Organizations and their owners must consider the implementation of a few standards and solutions to guarantee secure encrypted data management. The practices we introduce in

this subsection don't guarantee the secure encrypted data management per se, but they can help mitigate several weaknesses and mistakes that could lead to severely undesirable consequences that are historically difficult to recover. These practices make up a framework of good practices and standards that we recommend to be strictly followed by every organization, which is in control of private and sensitive data, especially if it is sensitive client personal data or payment information. Since these organizations are responsible for protecting such data, they must implement such measures to avoid exposing such data to be compromised. Organizations are legally and financially accountable if such sensitive data is compromised and they did not take the appropriate precautions.

Data Governance Frameworks

Governance frameworks exist to help organizations that handle sensitive data account for unique risks tied to their specific industry. Data governance frameworks define key terminology, establish a structure, mechanisms, and process to execute oversights and decision-making processes, and position your data governance function within your broader organization structure. Data governance frameworks have the following benefits. They can accelerate compliance. Data governance frameworks define data responsibilities and decision-making authority so that when compliance items arise, you know who is accountable and can act quickly.

5.10.1. Data Governance Frameworks

Data security and privacy risks can be reduced by creating and implementing data governance frameworks that clearly define who is responsible for ensuring the continual confidentiality, integrity, and availability of sensitive data for which the organization is custodial. These governance frameworks establish the set of guidelines, procedures, and assign specific data stewards, data guardians, data custodians, and data users/consumers for the entire data life cycle. Individuals assigned as data stewards are responsible for the conceptualization of data and rules governing its critical life-cycle stages, including its ownership, classification, quality, protection, sharing and dissemination, and retention, deletion, archival, or destruction. Data guardians are responsible for the physical and technical protections around the data, ensuring its compliance with all institutional policies and national/organizational rules and regulations governing the data pertaining to its confidentiality, integrity, and availability. Data custodians are responsible for the daily operations involving processing or working with the data. They are required to follow the security policies and guidelines put in place by the data steward and the data guardian. Finally, data users or consumers are individuals who are granted access to the data for the specific data-related tasks that they need to perform, merely following existing institutional, regulatory, and best practice security policies as needed.

Organizations could take an enterprise-level holistic approach through a cybersecurity operations center or data compliance team to serve as the data guardian group that serves the entire institution for all data access, sharing, and use. However, it is important to clarify that while there might be conceptual overlap in the roles of data steward, guardian, and custodian, each serves a very distinct function that is critical for the data governance and data operations workflows. In an institutional setting, these are considered important but decentralized responsibilities. The data steward would be the overall entity responsible for the classification of the sensitive data and the shared governance role for its accountability, policies, and compliance with respect to its use and sharing.

5.10.2. Regular Audits and Compliance Checks

Periodic audits and compliance checks are fundamental in identifying and resolving the latest security threats. An essential part of risk management, audits ensure that both internal and external controls are efficient and effective in reducing data breach risks. This is achieved by ensuring that the data is securely handled, accessed, or stored according to the organization's established data governance frameworks, data security standards relevant to the organization's sector, and the current laws and regulations. These documents specify the required criteria and best practices that must be implemented to optimally protect sensitive customer data. Furthermore, controlled access restrictions should be in place and enforced to allow only authorized individuals to access sensitive data.

Compliance checks and audits should also extend to third parties sharing confidential information for business operations. External entities such as cloud computing services used to hold or store encrypted data should also maintain compliance with local and international data compliance laws and mandates, which hold organizations accountable for securing private customer data. This is especially significant for companies not located in the same jurisdiction as the users whose data they are processing. Breaching laws or mandates can result in business closure and larger penalties such as jail time for the organization's executives. Moreover, organization executives are liable for any negligence in securing customer data. Failure to comply with data-sharing laws can also ultimately lead to loss of customer trust, negatively impacting the organization's reputation and fiscal performance.

5.11. User Education and Awareness

Cloud technologies have become primary data repositories for many organizations, making the need for user education and awareness more pressing. Every organization's

staff poses a security risk, intentionally or unintentionally jeopardizing the organization's cloud-enabled infrastructure. It is the responsibility of every employee to ensure that the protocols established to protect an organization from data breaches are stringent in practice as well as theory. Therefore, training programs for employees should be designed in a manner that the training becomes an integral part of both the onboarding process and the ongoing development in a broader sense. Employees should be aware of the security policies and determine which services are in use, how sensitive data is classified, and how machine learning algorithms can be used to automate some security processes. Cloud service providers should monitor the time employees use to access sensitive data. Moreover, employees should not hesitate to report security incidents or abnormal behavior that could indicate a potential breach. When responsible for securing sensitive data hosted in the cloud, employees must use two-factor authentication whenever possible and perhaps even physical tokens for extremely sensitive data. For the length of every password, the recommended number is at least twelve characters, using a mix of uppercase letters, lowercase letters, numbers, and special characters. Shorter passwords are vulnerable, especially if they are based on common phrases, so organizations that choose to permit their use could employ continuous updates. Employees should also be cautioned against using the same password for multiple accounts. Additionally, cybersecurity personnel in every organization should carry out periodic checks on all employees to determine if any ransomware strains already installed on employees' devices or if physical security expediently need patching.

5.11.1. Training Programs for Employees

This technical note covers training programs for employees who have been privy to the old way of using a legacy system. People are naturally resistant to change. A good case can be made for the protection of a legacy investment. Unfortunately, in many cases it is the investment made in people that is the greatest risk. When the day comes that the subject matter experts on a legacy mainframe are to retire, the company is seriously threatened because there is no one else who understands the system that is in place; no one else understands the investment made in the legacy system. When the legacy system is put to rest in favor of an enterprise-wide open-system solution, the enterprise can put those investments behind it for the future - if the enterprise has taken care of the user community; if the employees have been given sufficient training so they understand the new way. A legacy system works in a manner so different from a distributed environment that a one week quick-fix course will rarely make for a successful transition. Work on the ACM is reducing the cost and risk of education.

Learning from work is the methodology used to develop training programs for transitional education and update training programs for those areas of work where

continuous improvement is indicated. The idea is to populate training programs with procedural and informational content that is created from the ongoing work. The involved community designs the training program from their own experiences. They gather recently written reports that illustrate current processes. The involved community also describes differences in the way work was done in the past and the way it is done in the present.

5.11.2. Public Awareness Campaigns

While training is vital for organizations, not all security incidents come from within, but play a large part in economic espionage, identity theft, fraud, financial crime from external sources, and various other threats. In order to secure the digital economy, it is essential to also target the general public with awareness campaigns. These campaigns are of importance as they help to inform citizens about the existence of crime on the Internet, and how they can protect themselves from becoming victims. Especially the information age kids are often exposed to computer threats at an astonishing early age. They are using applications like Websites, e-Mail, Online-Gaming, and Chat Rooms, and are very excited about these. But while communicating and participating in these applications, they are at risk of becoming a victim of hacking attacks, fraud, or even sexual harassment. Therefore, they need to learn about how to use the Internet without putting themselves in danger. Sensitizing them alone at a very early stage of their Internet career would not have a beneficial effect. While this is very critical in retrospect, the importance of guiding the first steps of children as they enter the information technology jungle should not be neglected. Schools have a considerable amount of time for preparing the kids and therefore should work closely with public authorities in order to enable the public-key infrastructure for communicating securely. The main goal therefore is to create a population of users using the technology to the fullest by harnessing the educational efforts and protecting themselves from cyber threats at the same time.

5.12. Ethical Considerations in Data Management

Emerging technologies can help companies easily collect and analyze the massive amounts of data generated by different actors in various domains. Through a better understanding of this data, companies can improve decision-making, performance, and their value chain. As companies work to implement these technologies in their business strategies for major performance improvement, it is important to consider the ethical implications of data analysis in order to avoid potential negative consequences.

Data collection and management raise significant ethical and legal concerns about consumer privacy. Collected data can include usernames, passwords, credit card numbers, security codes, but also cookies that can be used to track websites visited by the user. Individuals whose data is collected and flagged for "undesirable" activities undertake significant risks. Moreover, on a larger scale, this data can be hacked and used to carry out criminal acts against individuals or groups within a demographic. Consequently, companies must be aware of where and how they collect data and what is done with that data after it is collected.

Individuals whose data is harnessed are also at risk for potential discriminatory practices that arise from "hidden biases" inadvertently incorporated into algorithms used to predict behaviors or actions within specific demographic groups. Discrimination cases surface when companies use certain data without input from individuals such as credit histories, criminal records, or medical histories unrelated to the desired action the algorithm is implemented to predict. As the ethical and legal guidelines surrounding data utilization within demographic groups are still appearing, companies utilizing these technologies must tread carefully.

5.12.1. Privacy Concerns

Nonetheless, privacy and security concerns bedevil the field of cloud computing. Privacy is a crucial building block of every community and a fundamental principle of a trustworthy digital and physical society, which is based on mutual respect. These concerns are not new. The problem of identity is as old as the concept of human civilization itself. In the digital arena – whether we are talking about cloud, big data, AI or the Internet of Everything – a person's identity is built on personal data. Citizens need protection against people or institutions that may have the power and resources to determine their identity and, on this basis, to infringe their privacy. If privacy is seen as a limiting factor that is of hindrance to innovation and competitiveness – denying economic and social developments to traders and customers, to service providers and recipients – these values must be balanced and appropriately safeguarded.

Furthermore, privacy is not just about protecting data but also controlling the information communication technology. Digital space seeks to offer privacy guarantees while enabling useful applications, enhanced social interaction and improved services for all participants in the digital community. The way privacy is managed must be adjusted to the proper context and, if needed, a selected group of users. Computer technology should use all available options and methods to not only grant privacy, but

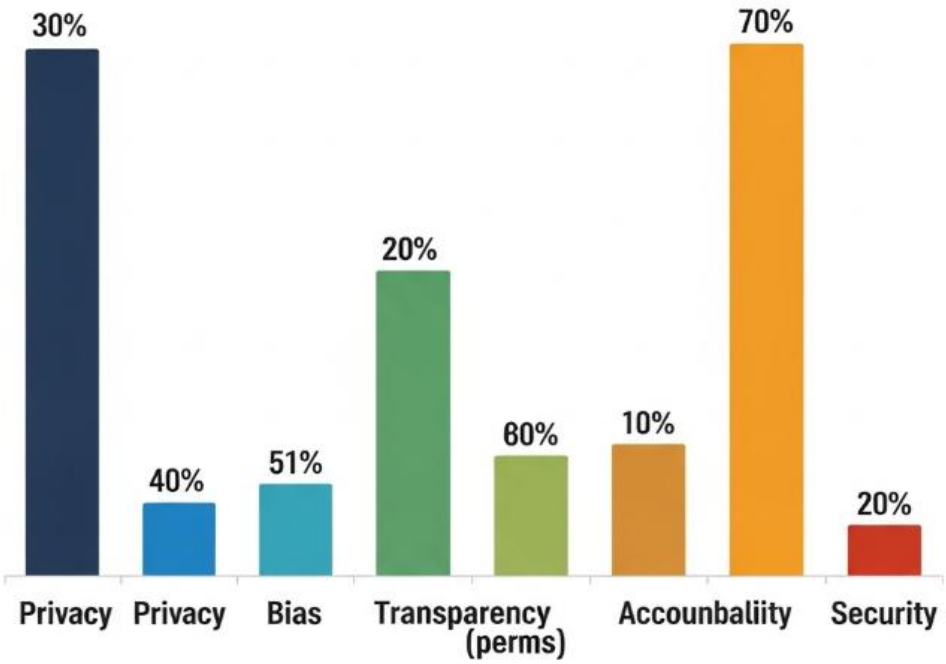

Fig : Ethical Considerations in Data Management

also transfer control of personal data and privacy back to users. Users should be offered advanced tools to manage sharing and discoverability of their profile, data and content. To a large extent, browsing and checking of the Service Level Agreement can mitigate security concerns, allowing choosing between providers that are encrypted, have a commitment not to spy and share data, and enable control access policies.

5.12.2. Responsible Data Use

In the rapidly evolving digital landscape, the use of sensitive data for app-assisted tasks has become commonplace. Online service providers offer advanced features such as speech recognition, photo filtering, and web personalization. However, these seemingly innocuous operations can often require access to private information such as user passwords, personal messages, and location history, raising ethical concerns about responsible data use.

The concept of responsible data use is a framework designed to share the burden of sensitive data handling with different stakeholders responsible for making corresponding decisions. Model designers establish the capability of their models and communicate it to the data owners. Data owners, typically collecting data from their customers, should

consider the potential detriment that may arise from the sharing of sensitive datasets that are ‘small’ in the sense that they may not be representative of their respective populations. At the same time, skilled model designers can, and may be required to, enforce rule sets on the retrieved templates so that they are only used for designated tasks. By working together, model designers and data owners can help to mitigate the risk of sensitive data breaches while still allowing for the development of advanced models trained on sensitive data.

5.13. Conclusion

Over the years, there has been a significant increase in cybercrime, which has increasingly exploited the opportunities offered by computerized and globalized financial infrastructure. As a result of these challenges, cloud computing and encrypted database technology has seen a rapid increase in highly-demanded financial services. The security of our financial system is vital for the economy, and thus it is crucial to ensure that it is sustainable in the future. We presented an overview of the history of Online Hot Wallets and their security problems, focusing on the solution to security problems and presenting new kinds of wallet architectures by combining cloud computing and hardware or paper wallet techniques. A first approach discussed the design of fast and simple internal Wallets by Cloud and Blockchain technology dedicated to facilitate small value transactions. It appears that combining blockchain technology and cloud computing offers a secure solution. The novelty of our approach is that cryptography should be adapted in order to offer the services required for using Hot Wallet architecture.

The perspective of this approach is to offer an infrastructure applicable to the computerization and adaptation of the security systems of the Financial systems. The use of such technology in both Private and Public exchanges could significantly reduce the opportunities for cybercrime to exploit security problems, as they do today. This would allow mobile and online services to have the necessary security and hence enable the development of this industry. The adaptation of such technology will ensure that there will be no chemistry nor real-world call or systems development, thus permitting that transactions statically are slow or don’t keep pace with technology of traditional Financial systems. In the near future, the solution presented could allow Blockchain solutions to be adopted in subsequent Cloud services and even become an alternative solution to Internally developed Financial Information Storage, thus permitting even such services to be made as hot as needed, without having to delay transaction sizing each time to avoid overflow.

References

N. Alexander, "Data Encryption Best Practices for Financial Data in the Cloud," Bob's Guide, 2025.

K. Roy et al., "Role of Encryption in Securing Cloud-Based Financial Data," ResearchGate, 2025.

S. Desai, "Encryption Techniques for Financial Data Security in Fintech Applications," IJERT, 2024.

C. Lefevre, "Client-Side Encryption and Secure Computation in Cloud Finance," AXA Research, 2024.

R. Zhang and Y. Liu, "Secure Model for Data Protection over Cloud Computing," NCBI PMC, 2022.