Considerations of Emerging Cloud Computing in Financial Industry and One-Time Password with Valet Key Solution

TE-YUAN LIN, CHIOU-SHANN FUH
Computer Science and Information Engineering
National Taiwan University
Taipei, Taiwan (R.O.C)
d03922002@ntu.edu.tw, fuh@csie.ntu.edu.tw

ABSTRACT

The services provided by the modern financial industry can date back to hundreds of years ago, which encompass a wide range of businesses relevant to money, including banks, insurances, stock brokerages, investment funds. The evolving cloud computing and big data technologies have brought big wave to the old economic activities. When the most conservative economic services come across the emerging cloud computing technology, there are both opportunities and challenges. This research is for those who concerned cloud computing security, considerations and solutions of the financial industry or for those limited cloud-acceptance organizations.

We propose a design called "Hybrid Cloud Architecture with OTP Valet Key Protection" based on the mixed deployment model to get a proper balance between the security concerns and the merits brought by the cloud computing. By keeping the data stored encrypted, cloud providers are prevented from peeking at the data content, validated users must acquire an extra valet key token after one-time password authentication to do any data access operations. This token is time-limited and even geo-limited according to custom policy. The entire token controlling procedure is under the financial administrator's arbitrations on the ground. The proposed scheme much eliminates the concern with data leakage while enhancing the whole system elasticity and scalability with cloud computing.

Through the case study, it enables re-considering the possibility of leveraging cloud paradigm even for the most conservative financial institutions.

KEYWORDS

Cloud computing; financial service; hybrid cloud; cloud security; banking; OTP; valet key token

1. INTRODUCTION

1.1 Topics in Financial Industry

In financial world, to facilitate the capital streaming is vital to the market share and success. People coming to the bank counter to deal with money is old-fashioned and too slow to the stream efficiency. Therefore, every banker is now gearing up for the big game of liquidity. This liquidity includes assets/capital liquidity (the ability and ease of converting to each other) and data/decision liquidity (the ability and speed of converting market data to right business decision and get feedback data from the result of decision made). *"Banking is no longer somewhere you go but something you do."* [1] just perfectly explained as it is. The interaction between customers will be changed, banks require the transformation in different service channels and models. To drive business growth and innovation, cloud computing seems to be the lighthouse of all the answers because of its potential advantages with capacity, elasticity, cost benefit, and easy of deployment.

"Compliance and Regulatory environments", "Mobile payments", "Cybersecurity" and "Big Data" are hot topics in financial industry — but all rely on increasing IT efficiency to achieve. The goal is to get closer to the customer, better maintain customer relationship, not just transactions. The key to the efficiency is cloud computing, it eliminates constraints around where physical IT resources are located or what specific technologies are employed, which makes it possible to deploy business services rapidly and at a lower cost, and touchdown for the goal.

1.2 Cloud Computing and Category

As soon as we discussed about cloud computing, the computing models and deployment objectives definition should be introduced as well.

According to the National Institute of Standards and Technology (NIST), the definition of cloud computing is composed of five essential characteristics**,** three service models, and four deployment models [2].

1.2.1 Essential Characteristics:

- *On-demand self-service.* A consumer can unilaterally provision computing capabilities, such as server time and network storage.

- *Broad network access.* Capabilities are available over the network and accessed through standard mechanisms.

- *Resource pooling.* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

- *Rapid elasticity.* Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand.

- *Measured service.* Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service.

1.2.2 Service Models:

- *Software as a Service (SaaS).* The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

- *Platform as a Service (PaaS).* The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

- *Infrastructure as a Service (IaaS).* The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

1.2.3 Deployment Models:

- *Private cloud.* The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g. business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

- *Public cloud.* The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them.

- *Hybrid cloud*. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability.

- *Community cloud.* The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns.

2. RELATED WORKS

2.1 Confidence of Ownership

In the scenario of on-premises, the ownership of every layer is in-house, from infrastructure, servers to middleware, data and applications. In the cloud-based scenario, as the abstraction level raises, the more managerial ownership of certain layers transfer to the cloud providers. Corporates need to find a balance between abstraction levels, costs, and security risks.

The abstraction level almost equals to the cloud adoption level. In the long term, higher cloud adoption brings more costs savings and business agility, however the effects of margin diminish, and the risk of ownership confidence increases instead. Here we use the term "the risk of ownership confidence" instead of "the risk of cloud adoption level" brings. Ownership transition to cloud vendors does not essentially bound to higher or lower risk, systems may be more steady and under world-class severe monitoring, but the ownership confidence to the corporate IT are affected. The risk of ownership confidence plays as the crucial determinant factor of the abstraction level, especially for bigger scale financial corporates. The risk of ownership transition to cloud vendors is usually considered higher to a greater extent, regardless of internally and externally.

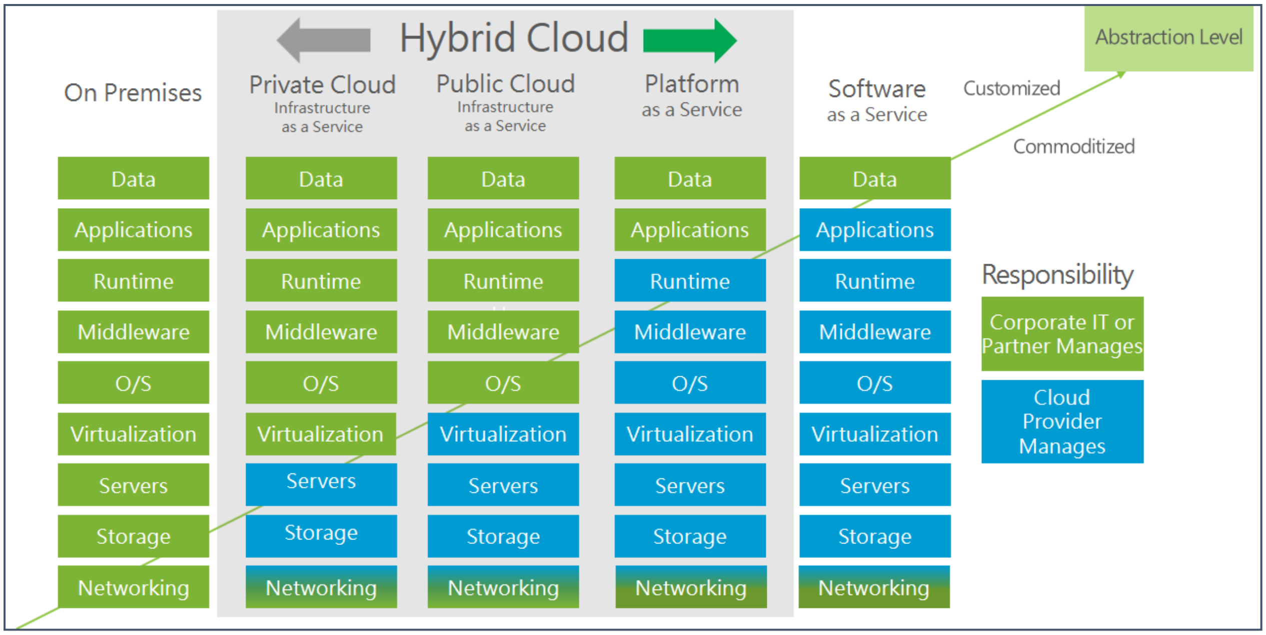
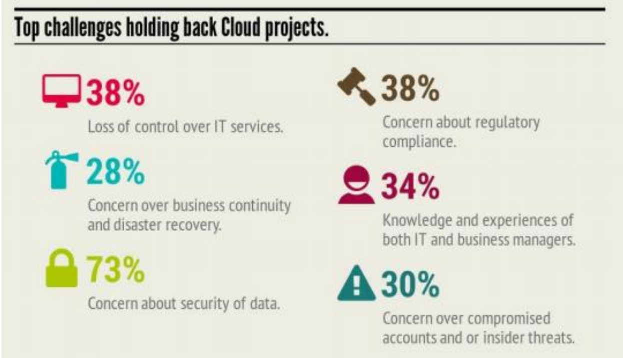


Figure 1. Cloud service models and managerial ownership [3].

To further analyze the risk challenges, according to the survey report result from Cloud Security Alliance (CSA), security & the control still remain the top barrier to cloud adoption.

Inferred from all the statistics, the mix of on-premises and cloud is the preferred adoption strategy, which is known as "Hybrid Cloud". Every layer in-house of financial corporates is allowed to be moving or at least duplicating to the cloud except security concerned data. Data security is the last mile of cloud adoption that is the economic artery to financial industry and never compromised.



Top challenges holding back Cloud projects.

38% Loss of control over IT services.

38% Concern about regulatory compliance.

28% Concern over business continuity and disaster recovery.

34% Knowledge and experiences of both IT and business managers.

73% Concern about security of data.

30% Concern over compromised accounts and or insider threats.

Figure 2. Top challenges holding back Cloud projects [4].

2.2 Security, Regulatory Restriction and Hybrid Cloud Strategy

In terms of security, since data privacy keeps a top barrier that holds the cloud computing adoption rate, one of the key strategies we advocate here is to help build better auditing, protecting and threat-analysis mechanisms throughout the cloud computing. It may sound like a contradiction, but think one step further, financial companies indeed feel more comfortable in enhancing data security and agility with cloud technology.

On the other hand, financial regulatory and compliance restrictions vary with countries, areas and markets. For instance, in Taiwan, Financial Supervisory Commission, R.O.C (Taiwan) [5] was established to supervise financial institutions and markets, including the banking market, bills market, securities market, futures and derivatives market, insurance market and their respective settlement systems.

Under its *Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation* [6], we can see specific instances of service level agreement and operational regulations of domestic banks and branches of foreign banks in Taiwan. Backup/ Recovery as a Service on cloud may be more meaningful here and worthwhile to consider.

Over the next years, financial institutes IT strategies will be increasingly impacted by the cloud, including reorganizing the IT department for closer cloud service brokering, redesigning new IT architecture for hybrid cloud interoperability, and redefining services roadmap for the execution plan applicability.

2.3 Cloud Solution Building Blocks and Considerations

Derived from cloud service models into major building blocks, shown in Table 1, it clearly expresses main features of cloud technology.

Most of the solutions can be built based on the combination of one or more building blocks. Certainly, these building blocks may increase or change as time goes by, it is an important characteristic of cloud computing.

Table 1. Building blocks of cloud solution.

SaaS	Web sites/web services provided by cloud vendors		
PaaS	Security & Identity	Database	Mobile Services
	Analytics	Content Delivery Network	Developer Services (SDK, Tools)
	Media Services	Cache	Workflow Services
	Web sites	NoSQL	Messaging
IaaS	Compute	Storage	Networks

Look deeper into the cloud solution composition, if we need a disaster recovery solution, the combination of database, web sites, networking service are indispensable, if we need analytical insights of big data, then storage, compute, and analytics services are the roles should be collaborating with one another.

No matter which deployment model, private cloud, hybrid cloud or public cloud, is all by integrating the set of functionalities above with on-premises or cloud environments. Before deciding any service provider and model, there are several questions and considerations to be considered:

- Legality: What do the financial compliances and regulations need to obey for offshore cloud computing?
- Agility and elasticity: Which provider (including our organization) offers the best technical architecture for our environment?
- Certification and Security: Which provider has attained third-party certifications and audits? (e.g. ISO/IEC 27001 [7]), IRS 1075 [8], or any standard that is highly recognized by our organization.)
- Innovation: Which provider (including our organization) has the best long-term product roadmap that meets our needs?
- Cost: What solution offers the best Total Cost of Ownership (TCO) over the next five years?
- Support: Help and support efficiency? Effective support options should at least include technical assistance via email, telephone and even onsite support for emergency.

- Experience: Any similar reference or experience from existing financial institution?

To pursue the absolute top ranking provider is not meaningful. However, after all the questions above were carefully answered, to choose the best suitable provider(s) that satisfy organizational status and needs is vital to financial IT successful transform.

3. PROBLEMS and METHODS

In financial industry, we all know the service activity fluctuation varies over time based on many factors. For the predictable usage, more users are likely to be active during business hours, and seldom active in weekends, but for others, like limited time promotion for credit card owners or marketing events make sudden bursts in website activity. Industrial news, political situation changes or economics changes can also bring unanticipated bursts in activity as well. We do not want to buy all the resource capacity of equipment just to meet the short peak demand. However, it is difficult to predict the load exactly as it will be. If the processing requirements exceed the system capacity, it will suffer from poor performance and even service down. Cloud computing has all the merits of cost and flexibility to the above-mentioned problems.

As a mean of common IT architecture in financial sectors, every endeavor in the traditional computing model is to prevent users from attack or invasion. Once we adopt cloud computing models, the security target remains the same, while the change is in administrative side with some loss of control over the infrastructural resources and some transferred ownership from administrators to cloud providers. How do we overcome the above limitations and utilize the cloud computing merits? In response to the transformation, IT administrator should adjust current infrastructure and role played from as-is whole-proprietary to hybrid-ready. Data, application and middle layer tiers should also be adjusted as well. For the security consideration, a feasible approach is to place the encrypted database instead of the original one in the cloud provider's environment. Additional procedures to decrypt or encrypt message before sending to users or storing to cloud data stores is inevitable. The permit of running additional operations relies on the valid valet key token issued after one-time password authentication which is followed by legal user's logon. The following sections will cover the key techniques used in our proposed scheme.

3.1 One-Time Password System

Strong one-time password systems can solve the vulnerability of memorable password problem and reply attack. There are many researches on one-time password system, generally, it can be classified into three types depending on password generation and authentication mechanism.

- S/Key Authentication

A typical one-time password mechanism that generates password authentication based on a finite hash chain which is generated by a secret key with software method. It does not save user's secret key on the authentication server and prevent from secret key leakage [9] [10]. However, the seed and iterative values of S/Key mechanism are in clear text over the network transmission, in addition, the mechanism is restricted by number of permissible authentication which is not suitable for multi-times authentications of registered users and strong secured requirements in our scenario. In our proposed scheme, we will leverage this unidirectional authentication model but use infinite hash chain to overcome the limitation.

- Challenge-Answer based Authentication

The challenge-answer scheme introduces additional calculating steps in handling the challenge to guarantee the issuance. The extra mathematical calculations are required for every transfer at both client and server, hence the performance is slower. The bidirectional challenge-response model may not be suitable to public user-facing scenario since the authentication server usually does not directly talk to the clients.

- Time-based Authentication

The authentication is based on the time-synchronization mechanism between the counter of server and client. The representative value from the time of client will be used as one of the input value of generating the server one-time password pair. However, the clock deviation, network and transfer time delay between the client and server are the connatural technical problems [11].

3.2 Valet Key Design Pattern

The concept of valet is an idea of agent for master with certain restriction. This concept comes in handy to the scenario when users need to manipulate the encrypted data and resources, in the meantime, without requiring the administrator to present the backend master key on the network.

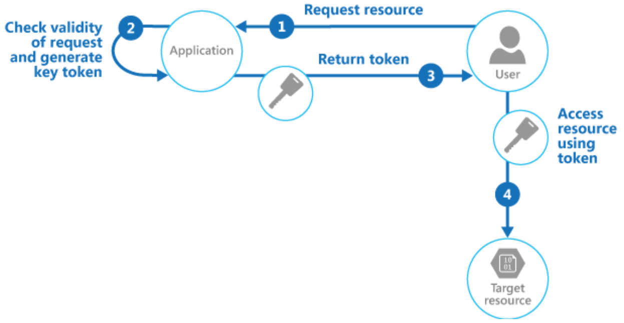

Request resource
1
Check validity of request and generate key token
2
Application
Return token
3
User
Access resource using token
4
Target resource

Figure 3. The Valet Key Pattern Overview [12].

Despite many advantages brought by this pattern, in our scenario, neither for minimizing resource load nor reducing the computing consumption on the application layer as listed in the reference, we intend to make the most use of integration with one-time password to solve the ownership and data store separation problem. We will depict more detail in later section.

4. OUR PROPOSED SCHEME

As stated earlier in this section, the resources and some ownership is transferred from on-premises administrators to cloud providers, especially the database. The user role has the user access credential and the data use right of his or her own, the cloud provider has the inventory space and computing power of the data without use right, and financial IT administrator has the ownership right of data and the permission control of user credential but may not physically store the data. Our proposed scheme is to design an architecture where every successful access to the data store must flow through these three roles, with the final decision held by financial IT's administrator.

By keeping the data store under public key protection of on-premises IT, the cloud provider has no chance to peep into database content and guarantee the safety. Any user who wants to operate data must acquire valid valet token in the predefined applications monitored by financial IT's arbitration. Figure 4 shows the overview of the proposed scheme process.

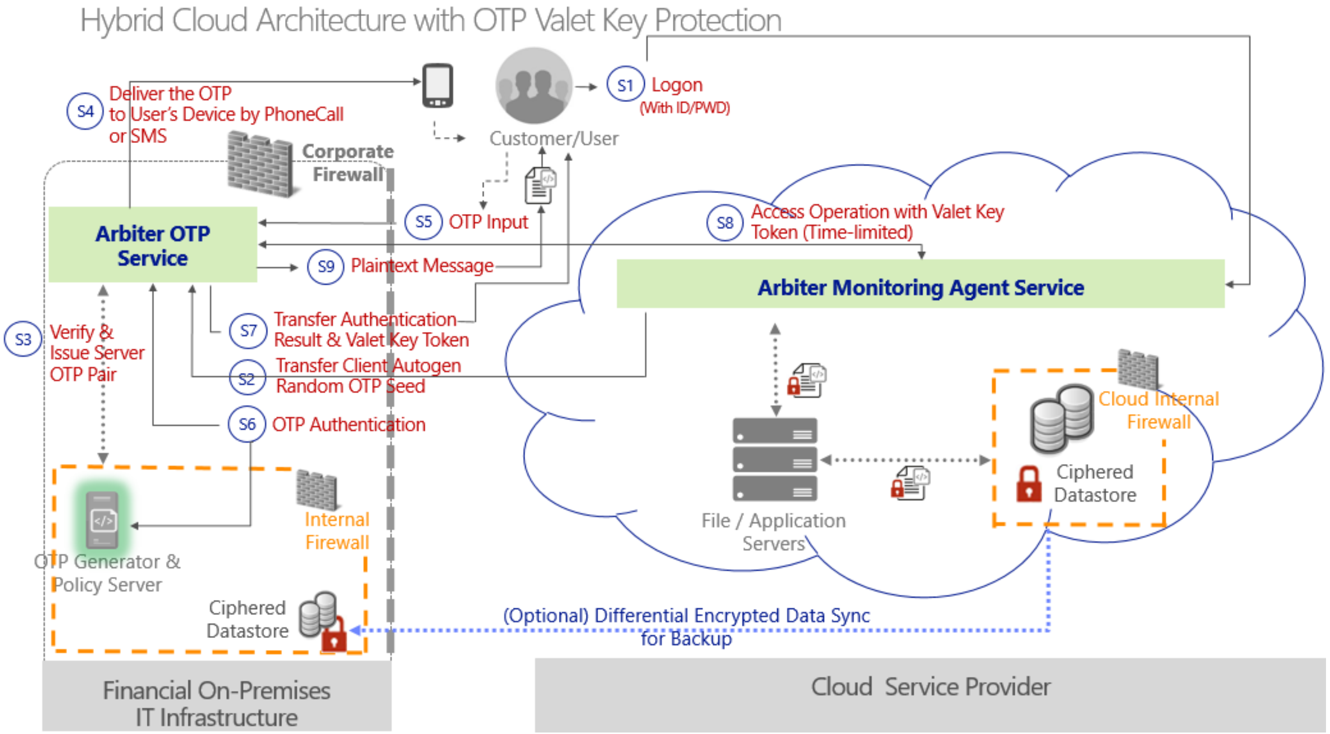

Hybrid Cloud Architecture with OTP Valet Key Protection
S1 Logon (With ID/PWD)
Customer/User
S4 Deliver the OTP to User's Device by PhoneCall or SMS
Corporate Firewall
S5 OTP Input
Arbiter OTP Service
S9 Plaintext Message
S8 Access Operation with Valet Key Token (Time-limited)
Arbiter Monitoring Agent Service
S3 Verify & Issue Server OTP Pair
S7 Transfer Authentication Result & Valet Key Token
S2 Transfer Client Autogen Random OTP Seed
S6 OTP Authentication
Internal Firewall
OTP Generator & Policy Server
Ciphered Datastore
File / Application Servers
Cloud Internal Firewall
Ciphered Datastore
(Optional) Differential Encrypted Data Sync for Backup
Financial On-Premises IT Infrastructure
Cloud Service Provider

Figure 4. Hybrid Cloud Architecture with OTP Valet Key Protection Overview.

- S1: User logs on with his/her own ID and password to the arbiter monitoring agent service.

- S2: Once the logon succeeds, the agent service generates client's one-time password (OTP_{cn}) based on the infinite hash chain on the runtime, redirects the user to financial IT's arbiter OTP service page and also transfers the generated OTP for n^{th} user from client side:

  $$OTP_{cn} (t) = A^{n} (t, e) \qquad (1)$$

  where t is the initial seed, and e is the public key of financial IT administrator.

- S3: Arbiter OTP service will verify the OTP according to predefined policy of the n^{th} user, if aligned with the compliance, then the Arbiter OTP Service issues server's OTP pair for n^{th} user of client side:

  $$OTP_{sn} (cn) = A^{n+1} (t, e) \qquad (2)$$

  where cn is $OTP_{cn} (t)$ in Equation (1)

- S4: Deliver the server's OTP pair to user's device by SMS or Phone call, and this is an independent channel from user's login operation.

- S5: User inputs the OTP sent from the financial IT on the Arbiter Monitoring Agent Service page and forward this to financial IT's Arbiter OTP Service.

- S6: The Arbiter OTP Service authenticates the OTP with Equation:

  $$A(OTP_{sn} (cn), d) = OTP_{sn} (OTP_{sn-1} (cn)) \qquad (3)$$

  where d is the private key of financial IT administrator.

- S7: Once the OTP is matched, the Arbiter OTP Service will generate a valet key and transfer this token to the user directly. S/he can start subsequent operations. The valet key token is designed to bound two dependencies simultaneously, one is on the comparison of one-time password and the other is predefined compound policies which can be set very flexible, such as time-limited to 60 seconds ~ several minutes, user's geo-location-limited, IP-limited, profile information and the scope of the data location. Server side reserves the privilege of invalidating published token at any time to promise the safety.

- S8: With valet key token, user can operate the data access, but since the content retrieved from the data store is still encrypted, the ciphered message needs to send back to the Arbiter OTP Service to decrypt by the Arbiter Agent. On the contrary, the plaintext from the user input also needs to send back to Arbiter OTP Service to encrypt and then be saved in data store.

- S9: User can see the plaintext message according to her own use rights.

For the reliability and backup reason, corporate might be required to keep a synchronized replica of the encrypted data store. The Arbiter Monitoring Agent Service and related applications can be rebuilt on-premises very quickly, and reconnect to the grounded-version of data store to recover the service in a short time.

5. CONCLUSIONS

The cloud computing and its advantage are prominent widely in many services, but the real adoption in financial IT infrastructure has not blossomed as expected. Data leakage and the loss of control risks are obviously the two obstacles to be named on the road. Especially migrating the whole sensitive databases to the cloud is highly concerned that every manager in financial services (as elsewhere) agrees. But think further, the fear of ownership loss that could lead to the trust challenges between cloud services consumers and providers are the real obstacles on the critical path.

In the beginning of this paper, we walked through the introduction of the cloud computing characteristics and models, followed by the essential considerations to the choice of adoption, and then proposed an architecture called "Hybrid Cloud Architecture with OTP Valet Key Protection" based on the mixed deployment model to get a proper balance between the security concerns and the merits brought by the cloud computing. The novelty of the solution designed is to enforce every successful data access request from the cloud must get the approval by the ground policy, guarantee the data confidentiality and prevent from cloud provider's possible peeking and tampering of data stores. The proposed scheme eliminates the doubt of placing sensitive database on the cloud.

REFERENCES

[1] Brett King, Bank 3.0: Why Banking Is No Longer Somewhere You Go But Something You Do. New York: Wiley, November 2012, pp. front cover.

[2] Peter Mell & Timothy Grance, The National Institute of Standards and Technology [NIST] Definition of Cloud Computing", National Institute of Standards and Technology, U.S. Department of Commerce, September 2011, Computer Security Special Publication 800-145.

[3] Yuri Diogenes, Best practices for software updates on Microsoft Azure IaaS. (2016, May 18) [Online]. Available: https://azure.microsoft.com/en-us/documentation/articles/azure-security-best-practices-software-updates-iaas/

[4] Cameron Coles, John Yeoh, Frank Guanco, Ekta Mishra, Luciano Santos, and Kendall Scoboria, "Cloud Adoption Practices & Priorities Survey Report,", United States, Cloud Security Alliance, January 2015, pp. 10.

[5] Financial Supervisory Commission, R.O.C (Taiwan). (2015). *The Financial Supervisory Commission (FSC)* [Online]. Available: http://law.fsc.gov.tw/law/index.aspx

[6] Financial Supervisory Commission, R.O.C (Taiwan). (2014, May 9). *Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation*. [Online]. Available: http://law.fsc.gov.tw/law/EngLawContent.aspx?Type=E&id=1327&KeyWord=%e9%87%91%e8%9e%8d%e6%a9%9f%e6%a7%8b%e4%bd%9c%e6%a5%ad%e5%a7%94%e8%a8%97%e4%bb%96%e4%ba%ba%e8%99%95%e7%90%86%e5%85%a7%e9%83%a8%e4%bd%9c%e6%a5%ad%e5%88%b6%e5%ba%a6%e5%8f%8a%e7%a8%8b%e5%ba%8f%e8%be%a6%e6%b3%95

[7] International Organization for Standardization. (ISO) (2013, Sep. 25). *ISO/IEC 27001* [Online]. Available: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[8] Internal Revenue Service. (IRS). (2014, Jan. 1). *IRS 1075* [Online]. Available: https://www.irs.gov/uac/Additional-Requirements-for-Publication-1075

[9] Nail M. Haller, "The S/Key One-Time Password System", *Proc. Internet Society Symposium on Network and Distributed System Security*, 1994, pp. 151-158.

[10] L. Lamport, "Password Authentication with Insecure Communication", *Comm. ACM*, vol. 24, No 11, 1981, pp. 770-772.

[11] Joong-gil Park, Tae-joo Chang, Bong-Joo Park, Jae-cheal Ryou, "An Effective One-Time Password Algorithm Using Time", *KIPS Journal*, vol. 8-C No. 04, 2001.08, pp. 0373-0378.

[12] Alex Homer et al., *Cloud Design Patterns: Prescriptive Architecture Guidance for Cloud Applications. Microsoft Patterns & Practices*, January 2014, pp. 160-165. [Online]. Available: https://www.microsoft.com/en-sg/download/details.aspx?id=42026