CLOUD COMPUTING DATA SECURITY IN CLOUD COMPUTING FOR BANKING

***Anand Tanvashi**
Assistant Professor
Surana College
Bangalore

****Shravani B**
Assistant Professor
Surana College
Bangalore

ABSTRACT

Cloud Computing has been anticipated as the next generation architecture of IT Enterprise. Cloud Computing moves the application software and database to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges. In this paper, we focus on cloud data storage security for banking, which has always been an important aspect of quality services in banking sector. To ensure the correctness of users' data in the cloud, we propose an effective and flexible solution.

As customers we do not need to own the infrastructure, Data can be redundantly store in multiple physical locations. Due to this redundancy the data can be easily modified by unauthorized users which can be stored in the database. This leads to loss of data privacy and security to database. Extensive security and performance analysis shows that the proposed scheme ensures that cyclicredundancy check and time-tested practices and technologies for managing trust relationships in traditional enterprises.These practices include data encryption, strong authentication and fraud detection, etc.

Keywords : Cloud Computing, application software, redundancy, data encryption, strong authentication and fraud detection

1. INTRODUCTION

Cloud Computing is one of the most impacting technology innovations today. It increases the flexibility scalability over internet.

To drive growth and innovation in banking, it is increasingly necessary to dramatically leapfrog the competition using IT and business model transformation. Google Wallet, Apple Wallet, PayPal and others are driving billion dollar revenues.

These established solutions have served the industry well, but problems now exist. Transaction volumes and regulatory compliance burdens also increase operational risk. The dramatic changes taking place in banking require new ways to maximize profitability and returns. By modernizing and transforming older back office systems into modular building blocks, banks can create a flexible and agile banking environment that can quickly respond to new business needs.

Cloud computing is revolutionizing ecosystems in multiple industries, and banking is no exception. Cloud technology offers secure deployment options that can help banks develop new customer experiences, enable effective collaboration and improve speed to market, all while increasing IT efficiency. Cloud adoption is growing rapidly because it can be made secure for banking transactions.

However, in developing or updating a bank's cloud strategy and infrastructure, it is important to keep security in mind and need to understand which delivery models are appropriate based on security and trust requirements with connecting systems.

As cloud computing provides unlimited infrastructure to retrieve and to store data and is stored at multiple location and due to redundancy data can be modified by unauthorized users. This leads to the loss of data. So security and privacy becomes the main issue in the cloud computing for Banking application. In this paper, we explore the advantages for banking with cloud computing, problem arises when using banking with cloud computing and some solution for that.

Characteristics of cloud computing

Here are the five main characteristics that cloud computing offers businesses today.[1]

On-demand capabilities : A business will secure cloud-hosting services through a cloud host provider which could be your usual software vendor. You have access to your services and you have the power to change cloud services through an online control panel or directly with the provider. You can add or delete users and change storage networks and software as needed. Typically, you are billed with a monthly subscription or a pay-for-what-you-use scenario. Terms of subscriptions and payments will vary with each software provider.

Broad network access : Your team can access business management solutions using their smartphones, tablets, laptops, and office computers. They can use these devices wherever they are located with a simple online access point. This mobility is particularly attractive for businesses so that during business hours or on off-times, employees can stay on top of projects, contracts, and customers whether they are on the road or in the office. Broad network access includes private clouds that operate within a company's firewall, public clouds, or a hybrid deployment.

Resource pooling : The cloud enables your employees to enter and use data within the business management software hosted in the cloud at the same time, from any location, and at any time. This is an attractive feature for multiple business offices and field service or sales teams that are usually outside the office.

Rapid elasticity : If anything, the cloud is flexible and scalable to suit your immediate business needs. You can quickly and easily add or remove users, software features, and other resources.

Measured service : Going back to the affordable nature of the cloud, you only pay for what you use. You and your cloud provider can measure storage levels, processing, bandwidth, and the number of user accounts and you are billed appropriately. The amount of resources that you may use can be monitored and controlled from both your side and your cloud provider's side which provides transparency.

1.1 CLOUD COMPUTING ARCHITECTURE

Cloud providers typically center on one type of cloud functionality provisioning: Infrastructure, Platform or Software / Application, though there is potentially no restriction to offer multiple types at the same time, which can often be observed in PaaS (Platform as a Service) providers which offer specific applications too, such as Google App Engine in combination with Google Docs.

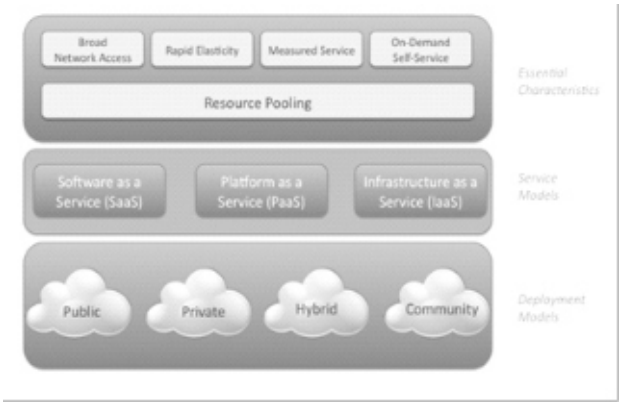

Fig1. Cloud computing architecture.

The following list identifies the main types of clouds :

Infrastructure-as-a-Service (IaaS) :

Infrastructure-as-a-Service is the first layer and foundation of cloud computing. Using this service model, one can manage their applications, data, operating system, middleware and runtime. The service provider manages bank application virtualization, servers, networking and storage. This allows bank applications to avoid expenditure on hardware and human capital and streamline and automate scaling.

Platform-as-a-Service(PaaS) :

This cloud service model could be considered the second layer. Users can manage their applications and data and the cloud vendor manages everything else. Benefits for using Platform-as-a-Service include streamlined version deployment and the ability to change or upgrade and minimize expenses. One popular Platform-as-a-Service is the Google app engine.

Software-as-a-Service(SaaS) :

This is the final layer of the cloud services model. This allows the business to run programs in the cloud where all portions are managed by the cloud vendor. The users will be assured compatibility and easier collaboration because all will be using the same software. Examples of this are online banking and email such as Gmail and Hotmail.

1.2 DEPLOYMENT MODELS

Public Cloud :

A public cloud infrastructure is available to the general public and is owned by a third party cloud service provider (CSP). In a public cloud, an agency dynamically provisions computing resources over the Internet from a CSP who shares its resources with other organizations.

To benefit from a public cloud, an agency must accept the reduced control and monitoring over the CSP's governance and security.

Private Cloud :

A private cloud infrastructure is operated solely for a single organization or agency: the CSP dedicates specific cloud services to that agency and no other clients. The agency specifies, architects, and controls a pool of computing resources that the CSP delivers as a standardized set of services. A common reason for agencies to procure private clouds is their ability to enforce their own data security standards and controls.

Community Cloud :

A community cloud infrastructure is procured jointly by several agencies or programs that share specific needs such as security, compliance, or jurisdiction considerations. The agencies or CSP may manage the community cloud and may keep it on-premises or off-premises.

Hybrid Cloud :

A hybrid cloud comprises two or more clouds (private, community, or public) with a mix of both internally and externally hosted services.

II PROBLEM STATEMENT

2.1 SYSTEM MODEL [2]

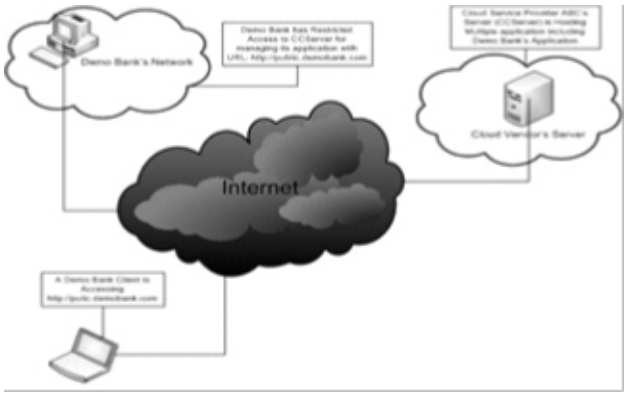

Fig2. cloud data storage architecture of banking

Banks are built on massive IT infrastructures that process huge volumes of data on a daily basis. The cloud's most obvious benefits will enable banks to keep up with technology changes, but concerns over a potential loss of control, availability and data security make moving to the cloud a massive leap in a heavily regulated sector.

Representative architecture for Data Storage for Banking Application using Cloud computing is illustrated in fig1.

Network entities identified are:

Demo bank client : Clients have stored their data in the cloud and rely on cloud for data security and computation for accessing Demo bank network through URL: http:/public.demobank.com.

Demo bank network : A secured network provider have expertise in data security navigation and is trusted to asses and uncover risks of cloud storage service on behalf of client/users.

CC Server – cloud service provider ABC's server (CC server) hosting multiple application including demo bank application. ABC Cloud Service Providers offer ABC Powered hybrid, private cloud solutions with stronger service-level agreements, better customer service, and proven expertise. Internet as Cloud which connects client, vendor and network.

A client/user stores his data through network into a server (CC Server) which is running in cooperated, distributed and real-time manner. Data security and redundancy can be implemented with a techniques including series of steps of Data Security Life Cycle (fig 2) to have the secured access to the bank cloud server through the network for fault tolerance or to handle server crash as user data accumulates and grows in size.

Fig3. Data security life cycle.

The client/user interacts with cloud server (CC Server) to access or retrieve his/her data. Sometimes the client may perform operations at different levels. The most general form of these operations considered are creation, insertion, updating, deletion and appending.

Clients no longer access data locally, it is important to assure users that their data is being correctly stored and maintained. To achieve this, the model Data Security Life Cycle is employed to secure the data so that they can make continuous correctness assurance of their data even without local copies.

In our model (fig 2) we assume that point to point communication channels between each cloud server and the user is authenticated at multilevel and reliable.

2.2 SECURITY THREATS

Security threats faced by cloud data storage in banking comes from the sources such as cloud service provider and paid adversaries such as hackers. Cloud service providers can be self-interested, malicious and untrusted. These may manipulate move data of client which may incur huge loss. And also it may lead malfunctioning of banking application itself. Some paid adversaries has the capability to compromise number of cloud data storage servers in different time intervals and able to modify, delete user data and user itself and other paid adversaries such as hackers may rename users and transfer data as well as content to some other client/user or to themselves without the knowledge of service providers, clients and cloud server.

Insecure Interfaces and APIs

Malicious Insiders

Unknown Risk Profile

Data Loss or Leakage

Account or Service Hijacking

III BEST PRACTICES : CLOUD DATA SECURITY LIFE CYCLE [3]

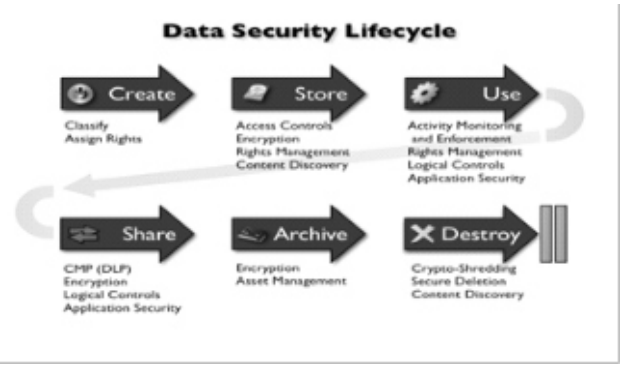

Fig 4.Cloud Data Security Life Cycle

CREATE : Create is defined as generation of new digital content, either structured or unstructured, or significant modification of existing content. In this phase we classify the information and determine appropriate rights. This phase consists of two steps – Classify and Assign Rights.

Classify

Classification at the time of creation is currently either a manual process (most unstructured data), or handled through application logic. Although the potential exists for automated tools to assist with classification, most cloud and non-cloud environments today classify manually for unstructured or directly-entered database data, while application data is automatically classified by business logic. These are the controls applied at the time of creation; additional controls such as access control and encryption are managed in the Store phase. There are two potential controls:

Application Logic: Data is classified based on business logic in the application. For

example, credit card numbers are classified as such based on field definitions and program logic. Generally this logic is based on where data is entered, or via automated analysis (keyword or content analysis)

Tagging/Labeling: The user manually applies tags or labels at the time of creation e.g., manually tagging via drop-down lists or open fields, manual keyword entry, suggestion-assisted tagging, and so on

Assign Rights

This is the process of converting the classification into rights applied to the data. Not all data necessarily has rights applied, in which cases security is provided through additional controls during later phases of the cycle. (Technically rights are always applied, but in many cases they are so broad as to be effectively non-existent). These are rights that follow the data, as opposed to access controls or encryption which, although they protect the data, are decoupled from its creation. There are two potential technical controls here:

Label Security : A feature of some database management systems and applications that adds a label to a data element, such as a database row, column, or table, or file metadata, classifying the content in that object. The DBMS or application can then implement access and logical controls based on the data label. Labels may be applied at the application layer, but only count as assigning rights if they also follow the data into storage

Enterprise Digital Rights Management (EDRM) : Content is encrypted, and access and use rights are controlled by metadata embedded with the content. The EDRM market has been somewhat self-limiting due to the complexity of enterprise integration and assigning and managing rights

STORE : Store is defined as the act of committing digital data to structured or unstructured storage (database vs. files). Here we map the classification and rights to security controls, including access controls, encryption and rights management. I include certain database and application controls, such as labeling, in rights management. Controls at this stage also apply to managing content in storage repositories (cloud or traditional), such as using content discovery to ensure that data is in approved/appropriate repositories

Access Rights :

One of the most fundamental data security technologies, built into every file and management system, and one of the most poorly used. In cloud computing environments there are two layers of access controls to manage – those presented by the cloud service, and the underlying access controls used by the cloud provider for their infrastructure, It has types

DBMS Access Controls : Access controls within a database management system (cloud or traditional), including proper use of views vs. direct table access. Use of these controls is often complicated by connection pooling. A database/DBMS hosted in the cloud will likely use the normal access controls of the DBMS. A cloud-based database comes with its own access controls. Depending on the security requirements, it is important to understand how the cloud-based DB stores information, so you can evaluate potential back-end security issues

Administrator Separation of Duties: Newer technologies implemented in databases to limit database administrator access. When

evaluating the security of a cloud offering, we need to understand the capabilities to limit both front and back-end administrator access. Many cloud services support various administrator roles for clients, allowing you to define various administrative roles for your own staff. You should ask your cloud provider (CS server) for documentation on what controls they place on their own administrators (and super-admins), and what data they can potentially access.

File System Access Controls : Normal file access controls, applied at the file or repository level. There are differences between the file accesses controls presented by the cloud service, vs. their access control implementation on the back end. There is an incredible variety of options across cloud providers, even within a single SPI tier (Saas, Paas and Iaas) – many of them completely proprietary to a specific provider Application and Document Management System

Access Controls: This category includes any access control restrictions implemented above the file or DBMS storage layers. In the cloud, this category includes any content restrictions managed through the cloud application or service abstracted from the back-end content storage. These are the access controls for any services that allow you to manage files, documents, and other 'unstructured' content. The back-end storage can consist of anything from a relational database to flat files to traditional storage, and should be evaluated separately

Encryption

For both enterprises using cloud environments and cloud service providers, encryption is a critical requirement for securing data files. Cloud Encryption provides the protection, encryption key management, fine-grained access controls and advanced security intelligence data to protect sensitive data-at-rest within public, private or hybrid cloud environments. . In cloud implementations, encryption may help compensate for issues related to multi-tenancy, public clouds, and remote/external hosting

Application - Level Encryption : Collected data is encrypted by the application, before being sent into a database or file system for storage. For cloud-based applications (e.g., public or private SaaS) this is usually the recommended option because it protects the data from the user all the way down to storage. For added security, the encryption functions and keys can be separated from the application itself.

Transparent Encryption : Media encryption is managed at the storage layer; never by the DBMS. Transparent encryption protects the database data from unauthorized direct access, but does not provide any internal security. For example, you can encrypt a remotely hosted database to prevent local administrators from accessing it, but it doesn't protect data from authorized database users.

Media Encryption : In a cloud environment, encryption of a complete virtual machine on IaaS could be considered media encryption. Media encryption is designed primarily to protect data in the event of physical loss/theft.

File/Folder Encryption : Traditional encryption of specific files and folders in storage by the host platform.

Virtual Private Storage is an effective technique to protect remote data when you don't have

complete control of the storage environment. Data is encrypted locally before being sent to the shared storage repository, providing complete control of user access and key management

Distributed Encryption : Distributed encryption helps with the main problem of file/folder encryption, which is ensuring that everyone who needs it gets access to the keys. Rather than trying to synchronize keys continually in the background, they are provide at need.

Rights management : The actual enforcement of rights assigned during the CRETE phase. For descriptions of the technologies, please refer to the CREATE phase. In future posts we will discuss cloud implementations of each of these technologies in greater detail.

Content discovery : is the process of using content or context-based tools to find sensitive data in content repositories. Content aware tools use advanced content analysis techniques, such as pattern matching, database fingerprinting, and partial document matching to identify sensitive data inside files and databases.

Cloud-Provided Database Discovery Tool : Your cloud service provides features to locate sensitive data within your cloud database, such as locating credit card numbers.

Database Discovery/DAM : Tools to crawl through database fields looking for data that matches content analysis policies

Data Loss Prevention (DLP)/Content Monitoring and Protection (CMP) Database Discovery : Some DLP/CMP tools support content discovery within databases; either directly or through analysis of a replicated database or flat file dump

Cloud-Provided Content Discovery : A cloud-based feature to perform content discovery on files stored with the cloud provider

DLP/CMP Content Discovery : All DLP/CMP tools with content discovery features can scan accessible file shares, even if they are hosted remotely

USE

Use includes the controls that apply when the user is interacting with the data – either via a cloud-based application, or the endpoint accessing the cloud service (e.g., a client/cloud application, direct storage interactionUsers interact with cloud data in three ways:

Web-based applications, such as most SaaS applications.

Client applications, such as local backup tools that store data in the cloud.

Direct/abstracted access, such as a local folder synchronized with cloud storage (e.g., Dropbox), or VPN access to a cloud-based serve

Activity Monitoring and Enforcement :

Activity Monitoring and Enforcement includes advanced techniques for capturing all data access and usage activity in real or near-real time, often with preventative capabilities to stop policy violations. Although activity monitoring controls may use log files. These first controls integrate directly with the cloud infrastructure:

Database Activity Monitoring (DAM) : Monitoring all database activity, including all SQL activity. Can be performed through network sniffing of database traffic, agents

installed on the server, or external monitoring, typically of transaction logs. DAM tools are managed externally to the database to provide separation of duties from database administrators (DBAs).

Application Activity Monitoring : Similar to Database Activity Monitoring, but at the application level. As with DAM, tools can use network monitoring or local agents, and can alert and sometimes block on policy violations. Web Application Firewalls are commonly used for monitoring web application activity, but cloud deployment options are limited.

File Activity Monitoring : Monitoring access and use of files in enterprise storage. Although there are no cloud specific tools available, these tools may be deployable for cloud storage that uses (or presents an abstracted version of) standard file access protocols.

Rights Management

The Create and Store sections explained the details of rights management.

Logical Controls : are implemented in applications and databases and add business logic and context to data usage and protection. The logical controls for the aspects of cloud computing, on data security includes:

Application Logic : Enforcing security logic in the application through design, programming, or external enforcement

Object (Row) Level Security : Object level security is a feature of the Database Management System and may or may not be available in cloud deployments.

Structural Controls : Structural controls are more widely available than object level security, and since they don't rely on IP addresses or external monitoring they are a good option for most cloud deployments.

Application Security : Effective application security is thus absolutely critical to protect data, and often far more important than any access controls or other protections.

SHARE

Share includes controls we use when exchanging data between users, customers, and bank. Where Use focuses on controls when a user interacts with the data as an individual, Share includes the controls once they start to exchange that data. In cloud computing we see a major emphasis on application and logical controls, with encryption for secure data exchange, DLP/CMP to monitor communications and block policy violations, and activity monitoring to track back-end data exchanges.

Network Data Loss Prevention/Content Monitoring and Protection : DLP/CMP

DLP/CMP uses advanced content analysis and deep packet inspection to monitor network communications traffic, alerting on policy violations. This can play multiple roles in protecting cloud-based data. In managed environments, network DLP/CMP policies can track (and block) sensitive data exchanges to untrusted clouds.

Encryption

Network/Transport Encryption : As data moves between applications, databases, the cloud, and other locations, the network connections should be encrypted using a standard network-layer protocol. Virtual Private Networks are useful for encrypting data moving in and out of clouds in certain deployment models.

Application Level Encryption : data encrypted by an application on collection is ideally protected as it moves throughout the rest of the application stack.

Email Encryption : since email is one of the most common ways of exchanging data, including reports and data dumps from cloud services, encryption is often relevant for cloud deployments

File Encryption and Enterprise Digital Rights Management : description of the encryption is given in store phase and share phase.

Logical Controls and Application Security are described in use phase.

ARCHIVE

Archiving is the process of transferring data from active use into long-term storage. This can include archived storage at your cloud provider, or migration back to internal archives.

From a security perspective we are concerned with two controls : encrypting the data, and tracking the assets when data moves to removable storage

CONTROL	STRUCTURED/APPLICATION	UNSTRUCTURED
Encryption	Database Encryption	Tape Encryption Storage Encryption
Asset Management	Asset Management	

DESTROY

Destroy is the permanent destruction of data that's no longer needed, and the use of content discovery to validate that it is not lingering in active storage or archives.

Organizations commonly destroy unneeded data, especially sensitive data that may be under regulatory compliance requirements. The cloud may complicate this if your provider's data management infrastructure isn't compatible with your destruction requirements (e.g., the provider is unable to delete data from archived storage). Crypto-shredding may be the best option for many cloud deployments, since it relies less on complete access to all physical media, which may be difficult or impossible even in completely private/internal cloud deployment.

Steps and Controls

CONTROL	STRUCTURED/APPLICATION	UNSTRUCTURED
Crypto Shredding	Enterprise Key Management	
Secure Deletion	Disk/Free Space Wiping	
Physical Destruction	Physical Destruction	
Content Discovery	Database Discovery	DLP/CMP Discovery Storage/Data Classification Tools Electronic Discovery

IV PROTECTION FROM FRAUD: UNAUTHORIZED ACCESS

Cloud providers have attracted enterprise customers with the promise of rapid elasticity, on-demand provisioning, high availability and a money-per-hour pricing model. But there's just one problem: These very qualities have enticed criminals to adopt cloud services as well.

When a hacker is looking to set up a phishing scheme to gain access to victims' bank accounts, the built-in redundancy, scalability and automation capabilities of cloud servers are

extremely appealing. And when all it takes to procure cloud services is a working credit card without ever needing to deal with a live salesperson, the cloud becomes an even more viable base from which criminals can commit fraud.

4.1 HOW DOES CLOUD-BASED FRAUD OCCUR?[4]

Across the broader market, discussions about cloud security have focused primarily on the customer side of the equation. Even as cloud providers continue to devote the resources necessary to ensure that customer data is secure, they can't overlook the fact that some of their own customers could be a threat.

Fraud manifests in the cloud in several ways, according to experts. Typically, fraudsters use a stolen credit card to procure virtual machine (VM) instances or platform services on which they build their operations -- among them phishing schemes, money-transfer scams, identity theft and malware.

Consequences of failure to detect fraud:Although fraud may not be the gravest security threat cloud providers face, ignoring it jeopardizes their bottom line in several ways.

From a purely financial perspective, any revenue gained from a stolen credit card is likely to evaporate quickly, thanks to the sophisticated fraud detection systems banks and credit card companies now use. The real damage comes from the revenues cloud providers never see from legitimate customers because the hundreds of VMs they would have paid to access have been tied up by the fraudsters.

4.2 DETECTING CLOUD FRAUD

Fraud detection and prevention is a real concern for cloud providers, which must balance customer privacy concerns with the need to snuff out illegal activities, according to John Howie, chief operating officer of the CSA (Cloud Security Alliance) and former head of data center security for a large cloud provider.

"Cloud providers have built up these very sophisticated, accurate and successful antifraud systems, and they've invested a lot of time and energy in it," Howie said. "They monitor how the customers use the service without monitoring their data instead, [they look] for patterns of activity that are indicators of [fraud]."

Once fraudulent behavior is detected, providers alert law-enforcement agencies and will even notify their competitors of patterns through anonymous forums the CSA hosts, Howie said. Sharing this information "has already developed very tangible results,"

As cloud security continues to evolve risk based authentication, which balances security, usability and cost by applying appropriate safeguards based on the risk associated with each activity, will undoubtedly play a major role in preventing fraud within both private and public clouds. In the coming years, organizations will need to extend their private cloud capabilities in strong authentication and fraud detection to protect against publishing, malware and even intellectual property theft. In building stronger defenses against unauthorized access and online fraud, organizations can borrow from the following fraud prevention practices pioneered by the financial services industry.

4.3 IMPLEMENT STRONG AUTHENTICATION SERVICES

Authentication is often the first line of defense in identity protection. Protecting users poses a challenge, as static passwords are considered too weak. Therefore, many cloud providers are actively seeking to implement a "better than password" authentication technology.

One of the most promising ways to secure online identities in the public cloud is risk based or adaptive, authentication systems, which intelligently vary authentication processes based on real-time calculations of risk. Risk-based identity protection employs behavior profiling and "invisible," or transparent, authentication processes in which users' requests for cloud services are compared with records of what those users have done in the past. Suspicious activities or patterns that deviate from the norm are automatically challenged.

Risk-based authentication methods are now being broadly deployed in many public clouds, particularly thoserun by financial institutions. For advanced risk-based authentication.

Processes, organizations further strengthen user authentication procedures by issuing security tokens to employees. Security token store inalterable, unique identities in protected memory on a small device. The tokens serve as secondary methods of verifying identities after users enter other Credentials, such as passwords or PINs. For enterprises to achieve consistent, guaranteed levels of identity protection, they need to push cloud services providers to deploy identity access and authentication tools that are equal in strength to those used in their enterprise.

V CONCLUSION

Cloud computiong offers real benefits to banking sector seeking the competative edge in today's economy. Many more providers are moving to this area. Just as there are advantages to cloud computing there are also several key security issues to be addresed. In this paper key security considerations and challenges which are currently faced in the cloud computing are highlighted.

Enterprises must have the ability to safeguard proprietary information on virtual servers and storage while giving cloud administrators the access and privileges needed to do their jobs. All of cloud issues relate to establishing trust relationships, which form the conceptual foundations for cloud security.

REFERENCES:

[1] http://www.ibm.com/developerworks

[2] http://www.jackcola.org

[3] https://securosis.com/blog/cloud-data-security-cycle

[4] http://searchtelecom.techtarget.com

[5] K. D. Bowers, A. Juels, and A. Oprea,"Proofs of Retrievability: Theory and Implementation," Cryptology ePrint Archive, Report 2008/175,2008, http://eprint.iacr.org

[6] G. Ateniese, R. Burns, R. Curtmola, J.Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. Of CCS '07, pp. 598–609, 2007.

[7] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Of SecureComm '08, pp. 1–10, 2008.

[8] T. S. J. Schwarz and E. L. Miller, "Store,Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," Proc.of ICDCS '06, pp. 12–12, 2006.

[9] M. Lillibridge, S. Elnikety, A. Birrell, M. Burrows, and M. Isard, "A Cooperative Internet Backup Scheme," Proc.of the 2003 USENIX

Annual Technical Conference (General Track), pp. 29–41, 2003.

[10] K. D. Bowers, A. Juels, and A. Oprea,"HAIL: A High-Availability and Integrity Layer for Cloud Storage," Cryptology