CLOUD SECURITY OR SECURITY IN BANKING

Vaibhav Kumar Pradhan,
Senior Manager
IT Audit, AU Small Finance Bank

DECLARATION: I AS AN AUTHOR OF THIS PAPER /ARTICLE, HEREBY DECLARE THAT THEPAPER SUBMITTED BY MEFOR PUBLICATIONIN THE JOURNAL IS COMPLETELY MY OWNGENUINEPAPER.IFANY ISSUE REGARDING COPYRIGHT/PATENT/ OTHER REALAUTHOR ARISES, THE PUBLISHER WILL NOTBELEGALLY RESPONSIBLE. IF ANY OF SUCH MATTERS OCCUR PUBLISHER MAY REMOVE MYCONTENT FROM THE JOURNAL WEBSITE. FOR THEREASON OF CONTENT AMENDMENT/OR ANYTECHNICLISSUE WITH NO VISIBILITY ONWEBSITE/UPDATES,I HAVERESUBMITTED THISPAPER FOR THE PUBLICATION. FOR ANY PUBLICATION MATTERS OANYINFORMATION INTENTIONALLYHIDDEN BYME OR OTHERWISE, ISHALLBELEGALLYRESPONSIBLE.(COMPLETE DECLARATIONOFTHE AUTHOR ATTHE LAST PAGE OF THIS PAPER/ARTICLE

ABSTRACT

Many companies and institutions now rely heavily on the Internet because of the rise of cloud computing. In order to meet their many needs and develop a banking system that can quickly adapt to changing market conditions, financial institutions are increasingly turning to cloud computing solutions. However, previous research has tended to look at the challenges of cloud computing adoption from the perspective of organizations, rather than the perspective of the people who actually utilize the services. So, this article aims to look into what customers think about cloud computing's impact on the banking industry and then offer an adoption strategy. TAM-DTM serves as the primary foundation for this model's development; three additional constructs—trust, cost, and security and privacy—are added to this model. A total of 162 Malaysian bank customers were sent out questionnaires at random. Partial least squares (PLS) analysis was employed to evaluate survey data, and SmartPLS was utilized for hypothesis testing and model validation. Based on the findings, it appears that TAM-TDM can accommodate trustworthy, cost-effective, secure, and private communications. Strong positive effects on usability, value, and confidence were observed for the security and privacy components. The discoveries of the review demonstrate that clients' conduct plan to take on distributed computing is fundamentally affected by factors like apparent value, saw convenience, cost, perspectives toward cloud, and trust. The results of this research will *help financial institutions better understand customers' viewpoints and feelings about cloud-based application adoption.*

Keywords: *Banking security, cloud security, the difficulties of cloud theory, and other related topics.*

1. INTRODUCTION

These types of changes in the financial industry have never before occurred. Today's environment is one where consumers, not banks, control the fate of financial organizations. The main focus of new business models is on the customer. Their use of technology, in addition to changes in social and household dynamics, is the main force behind the business world's revolution. Financial institutions must immediately update their business procedures, IT systems, and business models in order to adapt to this new, customer-driven environment. Banks will be able to combine a wealth of fragmented client information and analytics, and they will have a much better capacity to offer dependable service to customers across all of their branches and geographic locations. Financial institutions must take a step back and evaluate their activities from the perspective of their clients in order to bring about change in the banking industry. Due to the significant changes occurring in the banking sector, creative solutions to boost profitability and revenue are needed. Cloud computing offers secure deployment options that can aid banks in enhancing cutting-edge customer experiences, encouraging exceptional collaboration, and accelerating time to market while boosting IT efficiency. These advantages of cloud technology are in addition to its improvement in IT efficiency. The adoption of cloud computing has attracted more interest from a variety of industries, and the banking industry is no exception.

Financial institutions can create new markets and services thanks to the use of cloud computing, which makes them stand out from their competitors and increases the ways in which customers can access and use the products and services the financial institution provides. Banks that use cloud computing are well-positioned to meet the demands of clients with high expectations, universally integrated financial systems, and volatile financial markets. They can build more centralized offers that are in line with customer preferences using the information to better client segmentation tactics. Financial institutions can set themselves apart from rivals in a similar way by giving their clients better service and increasing their channel investments. Many businesses, including banks, are under pressure from the competitive nature of the modern economy to quickly adopt innovation into their current business structures. Financial service providers are among these businesses. Cloud computing, when applied to the banking sector, refers to two different types of end users. Because cloud services are advantageous to their operations and they already employ them, financial institutions are the first category of cloud consumers. The second classification of clients is the individuals who utilize the electronic apparatuses given by banks to deal with the ordinary pieces of their monetary lives. Monetary associations might establish a financial climate that is adaptable, speedy to answer changing business needs, and fit for doing so because of the utilization of distributed computing.

The banking and monetary administrations industry keeps on being of public significance and is pivotal to individuals' capacity to make a living since it straightforwardly helps the economy. Frameworks for exchange observing, tax evasion counteraction, and extortion identification are good to go up as a piece of the security execution in the specialized foundation of the bank. These controls take the form of browser protection guidelines, one-time password tokens, digital certificates for devices, and anti-fraud and money laundering detection systems. These contraptions and frameworks offer areas of strength for banks securities as well as stick to administrative necessities for safeguarding client information. Because of the boundless utilization of the web, organizations that arrangement with banking and monetary administrations have begun offering their items and administrations to clients by means of sites and mechanized teller machines (ATMs) in distant areas as opposed to by having them come into their actual workplaces.

These internet banking administrations increment the versatility and accommodation of admittance to banking administrations. For both retail and business clients, banks and other monetary foundations offer a huge swath of monetary labor and products. Web banking, versatile banking, ATM withdrawals and stores, Visa offices, check card offices, EFTPOS terminals, account the executives' administrations, financial exchange and depository items, and FX administration are a couple of instances of these labor and products. To utilize these administrations, you don't have to truly visit a bank office.

You can utilize the web to get to these things. Through faster help conveyance, lower branch working expenses, working with less staff individuals, offering serious administrations, settling on speedier choices for shoppers progressively, and zeroing in on their necessities, this helps banks in accomplishing functional effectiveness. Banking and monetary administrations are in congruity with national bank guidelines and norms because of cloud foundation. Information protection and frameworks security keep on being the top worry with no capacity to bear risk when the innovation foundation offering these types of assistance is situated at a got site and the two laborers and clients access it from different distant areas .

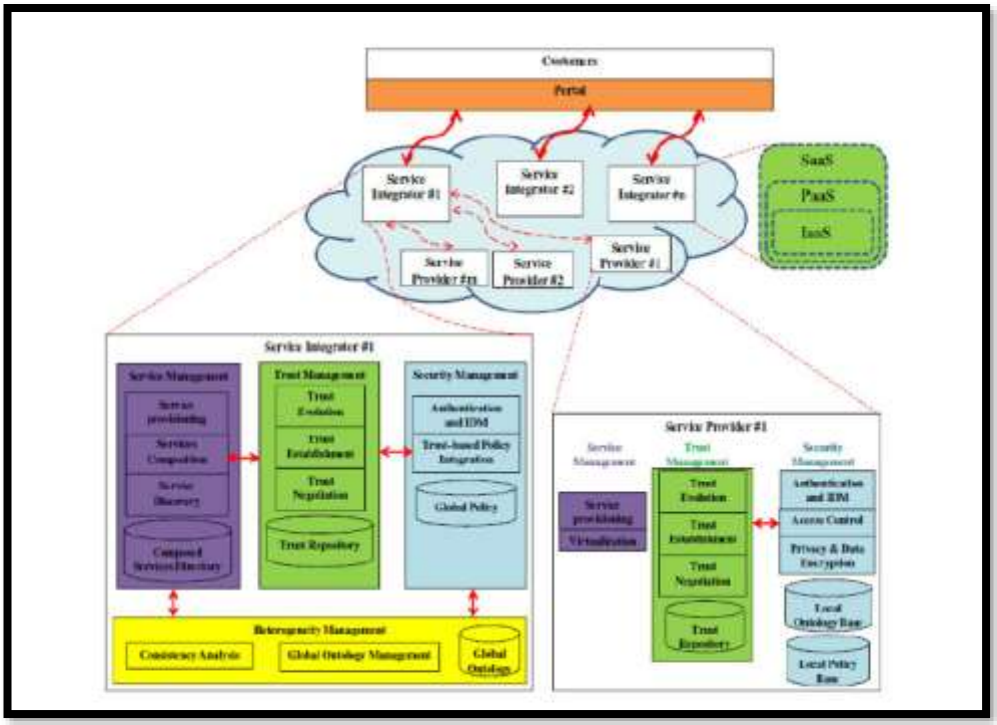


Figure 1: IDRBT Cloud Security Framework

It is expected to execute extra security, risk the board, and business congruity system to meet the prerequisites of getting distributed computing framework from possible risks and openings while at the same time keeping up with consistent openness for a great many clients. The expansion of information, the expanded utilization of cell phones, the far-reaching presence of informal organizations, the interconnection of different gadgets, and the different administrative standards in different nations all join to make the security system for cloud engineering much more complicated and dependent upon continuous assessment.

Furthermore, cloud innovation gives banks secure arrangement decisions, which can help them in the advancement of imaginative client encounters, the assistance of useful joint efforts, and enhancements in both the speed and productivity with which they can get to business sectors. Workers have the advantage of having the option to focus eagerly on the vision and objective of the bank subsequently. Moreover, this study presents applicable work on distributed computing, distributed computing in the financial business, an outline of the hypothesis that was used for this review, research approach, information examination and conversation of discoveries, as well as the issues that were confronted and the finish of the review.

2. LITERATURE REVIEW

Sangavarapu, et.al., (2014), With cloud computing, businesses can adapt quickly to changing market conditions and satisfy the needs of their customers. Organizations in the banking, financial services, and insurance industries are curious about cloud services as a technology, but only if they can be assured of security and privacy. A community cloud is one answer; in this setup, cloud services are provided to groups that have similar goals and security policies. The Institute for Development and Research in Banking Technology in Hyderabad, India, has launched the Indian Banking Community Cloud (IBCC) to meet the specific needs of Indian financial institutions on the cloud. This article provides an overview of the IBCC architecture, its implementation, the cloud services it provides, its security and disaster recovery measures, the difficulties encountered during deployment, and the plans for the future. This work is a contribution to a themed issue on the future of cloud computing.

Tiwari, et.al., (2021), Starting from its presentation empowered arrangements and administrations like Center Banking, Web based Banking, Portable Banking, Wallet, Wallets Booth Banking, banks have encountered a combination in their contacts with their end clients. Banks and their clients benefit from the expanded complexity of banking IT. The cutting-edge financial plan of action depends on satisfying clients through IT-empowered items and administrations. With the utilization of distributed computing, monetary organizations can embrace a computerized worldview to address the issues of their clients, consent to guidelines, and decrease the time it takes to put up new items for sale to the public. Cloud-based arrangements offer a more prominent offer to IT arrangements and administrations with regards to moving innovation standards. Gadget overseers utilizing cloud framework can remotely develop, transfer, tweak, and run virtual instruments to direct a business arrangement. Distributed computing additionally takes into account consistent versatility, meaning assets can be added or eliminated depending on the situation without disturbing assistance. The objective is to assess what distributed computing and artificial intelligence will mean for seriousness in business tasks and client support. The CFA strategy is utilized for affirmation. How well the quantity of develops is reflected by the deliberate factors and whether the assessment speculation is checked or dismissed are both displayed in the postulation.

Kshetri& N. (2012) Computing on the cloud is still in its infancy in India; but, as economic and institutional variables improve, cloud computing has the potential to greatly speed India's digitization and to transform how cell phones are used. The cloud has the potential to serve as a significant catalyst in promoting economic and social advancement and development in India, provided that the private sector and the government are able to produce products that are able to satisfy local needs and address difficulties such as low bandwidth and concerns regarding security.

Deshmukh, P. (2017), Most medical professionals have switched to EHR (Electronic Health Record) systems because they allow for more flexible data or record sharing. It's also helpful for nurses, doctors, and patients, among other people involved in the healthcare system. The cloud is becoming the backbone for most EHR because to cheaper costs and scalability of application without compromising data protection. In this study, we offer a framework for securing medical records and granting only authorized users (such as patients and doctors) access to them. The healthcare settings we've explored here—rural and urban clinics—are more suited to the needs of

Indians. By separating the transmission and storage encryption algorithms, the proposed scheme provides a higher level of data protection. The testing results demonstrate its scalability with respect to both the number of patients and the quantity of health record items.

Sattiraju, et.al., (2013, August) Cloud computing is an exciting new method of delivering on-demand services to consumers anywhere in the world with an Internet connection. Because of its simplicity, this technology is being adopted by more and more sectors around the world. Many businesses, including those in the business financial services industry (BFSI), are interested in exploring Public or Private Cloud services, but are hesitant to do so due to the security concerns surrounding this new technology. At the point when various organizations share comparative objectives and security strategies, a Local area Cloud might be the most ideal choice. The Save Bank of India's Establishment of Improvement and Exploration in Financial Innovation (IDRBT) has sent off an experimental run program to develop a Local area Cloud for Indian monetary foundations to use in offering IaaS. This archive portrays the IDRBT People group Cloud procedure for Indian banks, including its execution subtleties, undeniable level engineering, calamity recuperation plan, application appraisal preceding arrangement on the Cloud, network arrangements, and future turn of events.

3. PRIVACY AND SECURITY

3.1. Data Privacy

The term "data privacy" is used to describe how information shared with businesses is used. Data gathered by customers should be adequate to suit their business requirements and needs; consumers should accept the data; and customers should be given full transparency information. The Australian federal government has maintained penalties for companies that do not disclose sufficient information to their clients about data privacy. Personally Identifiable Information is the data collected in the banking and financial services industries that can be used to positively identify a customer.

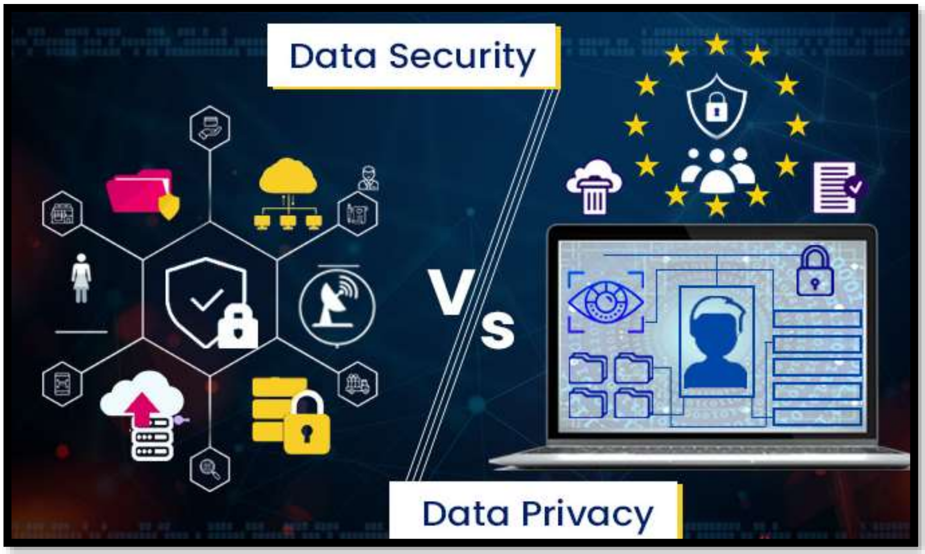


Figure 2: Data security and its privacy

3.2.Data Security

The terms "data security" and "data confidentiality" are often used interchangeably. Only approved parties have access to the data, and only they can see, modify, or delete it. When data is protected, it is always accessible, correct, and trustworthy. A well-thought-out data security strategy will ensure that only necessary data is collected, stored, and destroyed. Financial institutions continue to benefit from customers' right to privacy, and data security is the way through which this asset can be safeguarded for its intended use.

3.3.Information Privacy

The expression "data security" is utilized to depict individuals' assumptions for how much control they ought to have over private data. Protection, exactness, property, and openness (Dad) are four crucial worries in regards to the utilization of data that have emerged because of the advanced period. There are four features to security: physical, social, open, and enlightening. Because of the far reaching utilization of electronic mediums, for example, cell phones and the web, the once unmistakable ideas of individual correspondence protection and individual information security have merged into a solitary idea: data security.

3.4.Systems Security

The ability of a system to withstand assaults from the outside, whether they are malicious or unintentional, is referred to as its "security." They are made more reliable as a result of being dependable and available when necessary thanks to the secured systems. When secured systems perform as intended, without any failures or delays, they assist the banking and financial services business in accomplishing the goals it has set for itself.

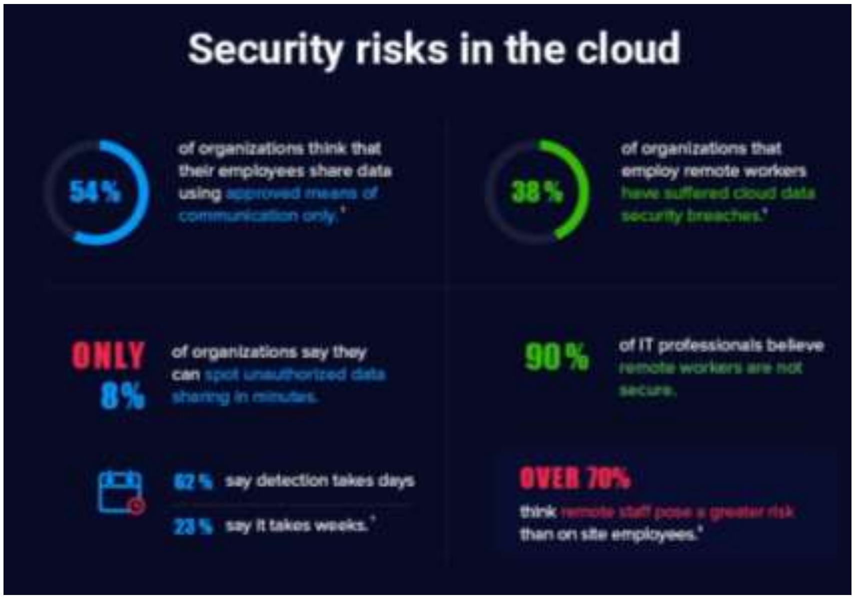
4. COMPROMISED SECURITY SYSTEMS WILL RESULT IN

4.1.DISTRIBUTED DENIAL OF SERVICES

Due to several infrastructure and network resource failures, service quality degrades or services become unavailable. Because of this, neither customers nor employees will be able to complete financial transactions or execute their jobs efficiently. This will cause widespread disruption to daily life and the economy. Due to the distributed nature of DDoS attacks, it is not always possible to identify their origins. As a result, it will take longer for systems to recover and resume regular operations.

4.2.TAMPERING (CORRUPTION) WITH SOFTWARE AND/OR DATA

Unapproved changes are made to information or potentially programs. There will be either monetary or functional misfortune, or both, contingent upon the idea of the adulterated programming (monetary handling, client information, capacity frameworks, interfacing gadgets, and so on.). A small measure of unseemly thinking in a product can essentially affect clients and representatives in the banking and monetary administrations business. There is a gamble that all monetary exchanges will be inaccessible on the web based financial stage assuming the site that empowers them is refreshed with new instructive connections and pages that utilization unseemly contents.



of organizations think that their employees share data using approved means of communication only.*

of organizations that employ remote workers have suffered cloud data security breaches.*

of organizations say they can spot unauthorized data sharing in minutes.

of IT professionals believe remote workers are not secure.

say detection takes days

say it takes weeks.*

think remote staff pose a greater risk than on site employees.*

Figure 3: Risks in the cloud system.

4.3.LEAK OF SENSITIVE MATERIALS

There is a gamble that unapproved gatherings will get sufficiently close to delicate information. A wide range of sorts of information are put away at banks and other monetary foundations. This data is put away on a common organization drive, consequently just approved clients ought to approach it.

Assuming that an unapproved individual was to erase these information, which either can't be held or the method involved with holding them takes an extensive time, it would straightforwardly affect the work that bank staff do.

Any break in the security of the framework might bring about the openness of chance to resources, misfortune (whether financial etc.), weakness to future assault or abuse, and loss of command over the framework. Controlling admittance to the actual framework is a fundamental piece of frameworks security, as is protecting the framework from possibly harming network access, code infusions, and information debasement.

5. THE MANAGEMENT OF INFORMATION SECURITY RISKS IN BANKING AND OTHER FINANCIAL SERVICES

When utilizing the architecture and infrastructure of cloud computing, banking and financial services take the following precautions to protect customers' personal information and privacy:

5.1.IDENTITY ACCESS MANAGEMENT:

This approach is useful for establishing the legitimacy of users and services using credentials and other identifying information. A "User Identity" (or a "Unique Network ID and Password") is an example of a credential, while "Characteristics" refers to a specified approach to managing cloud services. When customers' sensitive financial information and other personal details are stored in the cloud, it is crucial that only authorized individuals gain access to this data. By spotting users according to their duties and functions, IDM software helps to keep sensitive data safe.

5.2.MECHANISM FOR REGISTERING USERS AND REGISTERED ACCESS:

Cloud service delivery models have complex backend infrastructures. A policy-agnostic access specification and enforcement framework is required to integrate access control interfaces into this complex architecture. For the purpose of managing user access across many applications, the banking and financial services sector has embraced the Single Sign-On (SSO) approach. This access method performs a one-time authentication of the user's identification using "Single User Id / Network Id" and a password that complies with security rules. Access logging, also known as User Activity monitoring, refers to the practice of keeping track of and analyzing data about the users who access, operate, and maintain cloud infrastructure. All changes to data and applications may be tracked thanks to user activity monitoring in the cloud.

5.3.CONTROL OF ACCESS DEPENDING ON ROLES, AND BAD INSIDERS:

"Cloud computing" describes an approach to information technology in which several users share and make use of a shared pool of computing resources. It All Depends on Your Perspective The objective of access control is to guarantee that main approved people approach delicate data, and to fit that admittance to every individual's work capability. Role-based access restrictions are crucial for avoiding unintended or intentional disclosure of private information. A malevolent insider is a user who can access a system but lacks the credentials to perform adequate authentication or manage the system's use. When a user with administrative access steals private information, it is called "data theft." Factors in ensuring the security of private firm information include access restriction and management of potentially damaging insiders.

5.4.ADMINISTRATION AND CONFORMITY:

Leadership, organizational structure, and information-safety practices make up what is known as "cloud security governance." To be "compliant" is to meet the standards set out by the relevant government regulatory authorities. System strategic alignment with consumer, business, and employee needs is maintained through governance and compliance. The banking and finance industry's Governance and Compliance division provides a comprehensive operational, monitoring, metric, and communication structure with the purpose of keeping cloud architecture safe.

5.5.ADMINISTRATION LEVEL ARRANGEMENTS AND AGREEMENTS WITH CLOUD SPECIALIST ORGANIZATION:

The distributed computing foundation empowers on-request admittance to a common pool of far off servers. Cloud administrations should be painstakingly checked and kept in control to satisfy these particulars. Since cloud specialist co-ops can be found everywhere, global agreements frequently include the laws of more than one country. These arrangements ought to mirror the necessities of the client utilizing the cloud. To guarantee the wellbeing of different clients' confidential data, these agreements should perceive information protection and information security related concerns. In light of the significance of cloud administrations to the effective working of banking activities, SLAs and legally binding arrangements are progressively being viewed as fundamental for the outcome of these administrations. Administration level arrangements (SLAs) help in characterizing response time to be satisfied and reaction methodology to be done when issues emerge during customary business hours and beyond business hours. Administration Level Arrangements (SLAs) ensure that intruded on cloud administrations will be fixed inside foreordained times or have to deal with monetary damages. In this methodology, the monetary area can make up for misfortunes caused because of margin time. Authoritative arrangements effectively guarantee that, in case of information robbery or different breaks of information security related approaches, proper measures are taken to forestall extra mischief or information misfortunes.

5.6.SECURE DELETION OF DATA:

When their purpose is met, financial institutions destroy the data they've collected. Deleting old files is a necessary operational step in maintaining enough available storage for incoming data. To prevent any potential abuse or manipulation of data stored in the cloud and accessed by users, it is crucial that this data can be deleted in a safe manner. Since a third party manages cloud infrastructure, it is crucial to check that deleted data is truly gone and cannot be restored. Customer information that has not been erased may be used in the future to create fraudulent accounts and identities. The result will be an increase in financial crime and additional difficulties in establishing trust in cloud computing. Protecting data through secure deletion is essential.

Figure 4: Deleting of data

5.7.FORENSIC CAPABILITIES:

In the event of a financial crime, forensic capabilities allow the retention of data from system storage devices for further investigation and the production of said devices to satisfy legal need. Since the bank's cloud infrastructure is internal, getting permission to view logs from storage devices is less of a hassle. In addition, the cloud service provider agrees in written contracts to fulfill these needs of financial institutions.

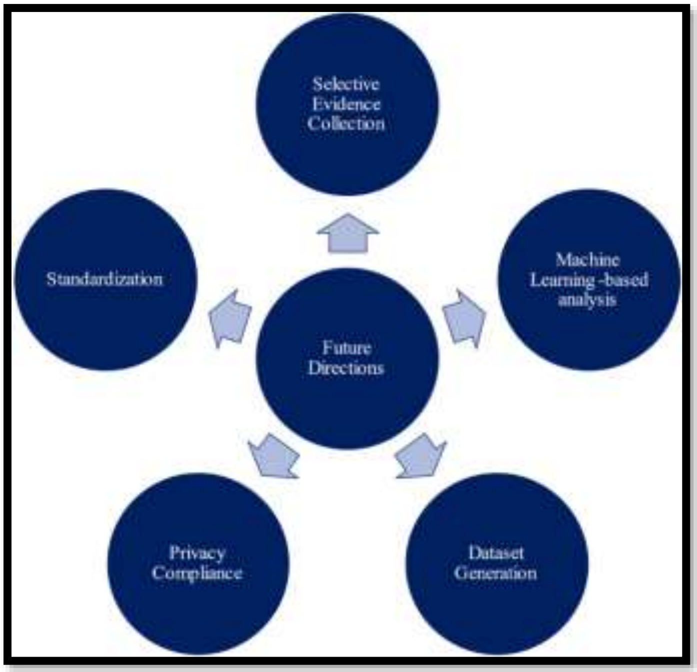


Figure 5: cloud forensic

5.8.COMPUTING IN THE CLOUD AND OUTSOURCING:

Cloud servers used by financial institutions should be located within the country's borders. Users of cloud services, however, typically work from afar. It can be more cost-effective to outsource users who are responsible for managing cloud services and data. However, an identity access management system is necessary to oversee these customers. There could be a number of different people with access to the system and data, depending on who those users are and how often they log in. It's possible that banks and financial institutions will lose control over these customers. Banks and other financial institutions observe the terms of their contracts with the companies that manage their cloud services and take all necessary measures (whether legal, disciplinary, or punitive) in the event of a security breach.

6. CONCLUSION

Distributed computing has diminished the expense expected to oversee IT foundation by fostering a strong and secure design. Nonetheless, for foundations like banks and monetary administrations that have clients' and organizations' monetary information, the cloud-based model brings long haul dangers and dangers of possible misfortunes because of unsure or unfavorable circumstances. Banks and other monetary establishments frequently utilize committed IT security groups to plan and execute their security foundation, yet this system should be routinely surveyed and refreshed to represent new dangers and different elements. Banks and other monetary associations keep on focusing on cloud security on account of the great gamble of outside assaults on their data frameworks.

REFERENCES

1. *"SP360: Service Provider: From India to Intercloud". Blogs.cisco.com. Retrieved 2010-08-22.*
2. *Ackermann et. al. / "Perceived IT Security Risk of Cloud Computing, 33rd, p.3, International Conference on Information Systems, 2012.*
3. *Agarwal NK (2011) Verifying survey items for construct validity: A two-stage sorting procedure for questionnaire design in information behavior research. Proc Am Soc Inf Sci Technol 48(1):1–8/*
4. *Aitenbichler E, Behring A, Bradler D, Hartmann M, Martucci L, Mu¨hlha¨user M et al (2009) Shaping the future internet. In: Proceedings of the 3rd international companionable workshop IoPTS.*
5. *Ajzen I, Fishbein M (1980) Understanding attitudes and predicting social behavior. Prentice-Hall, INC, Englewood Cliffs, NJ.*
6. *Alam, M., & Khokhar, R. (2006). Impact of Internet on Customer Loyalty in Swedish Banks. J. Econ. Psychol. Apr 7;16:311-29.*

7. Ardito, L., Petruzzelli, A. M., Panniello, U., & Achille, C. (2019). Towards Industry 4.0. Business Process Management Journal , Bradford Vol. 25, Iss. 2, pp: 323-346.
8. Awad, R. (2011). Considerations on Cloud Computing for CPAs. The CPA Journal , New York Vol. 81, Iss. 9, Sep pp: 11-12.
9. Canada (2007-11-29). "Head in the clouds? Welcome to the future". The Globe and Mail. Toronto. Retrieved 2010-08-22.
10. Deshmukh, P. (2017). Design of cloud security in the EHR for Indian healthcare services. Journal of King Saud university-computer and information sciences, 29(3), 281-287.
11. Foley, John. "Private Clouds Take Shape". InformationWeek. Retrieved 2010-08-22, p2-p14.
12. Hassan, Qusay F.; Riad, laa M.; Hassan, Ahmed E. (2012). "Software reuse in the emerging cloud computing era". In Yang, Hongji; Liu, Xiaodong. Understanding Cloud Computing (PDF). Hershey, PA: Information Science Reference. pp. 204–227. ISBN 978-1-4666-0897-9. doi:10.4018/978-1-4666-0897-9.ch009. Retrieved 11 December 2014.
13. Information Security Framework for Indian Banking Industry. IDRBT,
14. Kshetri, N. (2012). Cloud computing in India. IT professional, 14(5), 5-8.
15. Peter Mell and Timothy Grance (September 2011). The NIST Definition of Cloud Computing (Technical report). National Institute of Standards and Technology: U.S. Department of Commerce, p2-p3, NIST Special publication, September 2014.
16. Rouse, Margaret. "What is public cloud?" Definition from Whatis.com. Retrieved 12 October 2014, p1-p13.
17. Sangavarapu, L., Mishra, S., Williams, A., & Gangadharan, G. R. (2014). The Indian banking community cloud. IT Professional, 16(6), 25-32.
18. Sattiraju, G., Mohan, S. L., & Mishra, S. (2013, August). Idrbt community cloud for indian banks. In 2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 1634-1639). IEEE.

19. *Tiwari, S., Bharadwaj, S., & Joshi, S. (2021). A study of impact of cloud computing and artificial intelligence on banking services, profitability and operational benefits. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(6), 1617-1627.*
20. *Zissis D, Lekkas D (2012) Addressing cloud computing security issues. Future Gener Compute Syst 28(3):583–59.*

Author's Declaration

I as an author of the above research paper/article, hereby, declare that the content of this paper is prepared by me and if any person having copyright issue or patentor anything otherwise related to the content, I shall always be legally responsible for any issue. For the reason of invisibility of my research paper on the website/amendments/updates, I have resubmitted my paper for publication on the same date. If any data or information given by me is not correct, I shall always be legally responsible. With my whole responsibility legally and formally I have intimated the publisher (Publisher) that my paper has been checked by my guide (if any) or expert to make it sure that paper is technically right and there is no unaccepted plagiarism and hentriacontane is genuinely mine. If any issue arises related toPlagiarism/GuideName/EducationalQualification/Designation/Addressof my university/college/institution/Structure or Formatting/ Resubmission /Submission /Copyright /Patent /Submission for any higher degree or Job/Primary Data/Secondary Data Issues. I will be solely/entirely responsible for any legal issues. I have been informed that the most of the data from the website is invisible or shuffled or vanished from the data base due to some technical fault or hacking and therefore the process of resubmission is there for the scholars/students who finds trouble in getting their paper on the website. At the time of resubmission ofmy paper I take all the legal and formal responsibilities, If I hide or do not submit the copy of my original documents (Aadhar/Driving License/Any Identity Proof and Photo) in spite of demand from the publisher then my paper may be rejected or removed from the website anytime and may not be considerfor verification. I accept the fact that as the content of this paper and the resubmission legal responsibilities and reasons are only mine then the Publisher (Airo International Journal/Airo National Research Journal) is never responsible. I also declare that if publisher finds any complication or error or anything hidden or implemented otherwise, my paper maybe removed from the website or the watermark of remark/actuality maybe mentioned on my paper. Even if anything is found illegal publisher may also take legal action against me

Vaibhav Kumar Pradhan