IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 7, Issue 1, July 2021
Impact Factor: 4.819

Impact of Cloud Computing on Banking Sector, Its Security and Future Trends.

Ankita Anil Dhuri and Anjali Santosh Mane
Students, Master of Computer Application
Late Bhausaheb Hiray S.S Trust's Hiray Institute of Computer Application, Mumbai, India

Abstract: *Government of India initiative of Digital India has encouraged banks and other financial organisations to adopt cloud computing. Because of which; Cloud Computing has seen a substantial amount of growth in every sector. Many government sector & Private sector organisations have started using cloud computing as a preferred medium for storage and analyse data which can accessed from anywhere and at any time. Cloud computing has reduced the cost of management of physical & technical Infrastructure at the same time. Banking sector has specifically seen much development after accepting cloud computing as a medium to store data, Analyse security framework & maintaining privacy at the same time. With an adoption of cloud computing, banking services industry continues to be under strict regulatory and compliance framework to maintain privacy of data and security of systems. In this document we are going to learn about cloud computing and its impact on Banking sector. Along with that we are going to understand some future trends of cloud computing with respect to banking sector.*

Keywords: BLDC, ZETA, MPPT, PV

I. INTRODUCTION

1.1 What is Cloud Computing?

The term cloud Computing, the word cloud is analogy for the internet. The word cloud is inspired from the old symbol of cloud which was often used to represent to internet in flow chart. Through cloud computing, information systems resources that include application, data, network, storage devices and servers are made accessible and available for use.

A traditional set up will require you to be at the same place as your storage device. Cloud computing makes it easier to access the data anywhere and at any time. The cloud removes the need for you to be in the same physical location as the hardware that stores your data.

Cloud computing can be defined as a system for enabling convenient demand network access to a shared on-pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

1.2 Types of Clouds

There are different types of clouds that can consider for use depending on client's needs.

1. **Public cloud** - a public cloud can be accessed by anyone with an internet connection and access to the cloud space.
2. **Private cloud** - a private cloud is established for a specific group or organization and limits access to just that group.
3. **Community cloud** - a community cloud is shared among two or more organizations that have similar cloud requirements.
4. **Hybrid cloud** - a hybrid cloud is essentially a combination of at least two clouds, where the clouds included are a mixture of public, private, or community.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 7, Issue 1, July 2021
Impact Factor: 4.819

1.3 Different Cloud Service Provider

Each cloud service provides you with specific functions which give client a control over the cloud depending on the type of provider have been chosen. There are three types of cloud Service providers:

1. **Software as a Service (SaaS)** - a SaaS provider gives Client access to both resources and applications. SaaS makes it unnecessary to have a physical copy of software to install on your devices. SaaS also makes it easier to have the same software on all of your devices at once by accessing it on the cloud. In a SaaS agreement, client has the least control over the cloud.
2. **Platform as a service (PaaS)** - a PaaS system goes a level above the software as a service setup. A PaaS provider gives Client access to the components that they require to develop and operate applications over the internet.
3. **Infrastructure as a service (IaaS)** - an IaaS agreement, as the name states, deals primarily with computational infrastructure. In an IaaS agreement, the subscriber completely outsources the storage and resources, such as hardware and software that they need.

1.4 Types of Cloud Operating Models

Right cloud service model requires a proper cloud operating model which gives a mixture of proper Assets & resources. Cloud operating model can be of following types:

1. **Staff Augmentation** - Organisations can gain cloud expertise by cloud professionals with the right skill sets from cloud service Provider. This operating model allows organisations to choose thebest resource for each specific requirement.
2. **Virtual captives** -Virtual captives have a dedicated personnel or centres to help with cloud operations and meet demand.
3. **Outsourcing vendors** -This approach uses personnel working from outside the organisations, and people from a third party vendor to handle cloud operations. The model combines resources and investments to cater to cloud services

II. Impact of Cloud computing in Banking Sector

Banks has many reasons to migrate to cloud computing. Some of the major reasons are explained below. Less hardware & storage facility since data can be stored and used directly through internet & Virtual service. Cloud computing delivers computing power as a virtual service a product which benefits, software and computers and other devices as a utility on a shared network.

1. **Reduce cost:** major advantage of cloud computing is no usage of on-site hardware storage. Banks need not to use actual hardware and reduce IT Cost. Banks can just buy a subscription from Cloud Service provider & use it; making an actual hardware & IT personnel redundant.
2. **Business process improvement:** Cloud computing & Storage access provides readily available data whenever required by client. The technology workload between processor and server is highly reduced leading to proper resource management.
3. **Simplicity:** Cloud computing is simple to use and set-up all the services with no worries about resource management and other problems that come with infrastructure set up and management.
4. **Reliability:** Network and data access are guaranteed to be reliably maintained as the service provides are experts in maintaining the infrastructure
5. **Flexibility:** Clients have the flexibility to “outsource” parts of the infrastructure and can still maintain to some extent proprietary data at their own site.
6. **Privacy and Security:** Cloud computing allows users to add more capacity, more services and seamless software patches, despite of existence of encryption and access-control software.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 7, Issue 1, July 2021
Impact Factor: 4.819

7. **Data segregation:** A cloud is a shared environment in that data can be shared. There is the danger for data loss. Service provider needs to ensure that there is encryption available at all phases, and were these encryption patterns designed and tested by experienced professionals.
8. **Recovery:** It is very essential to recover the data when some problem occurs and creates failure. The main question arises here is that can cloud provider restore data completely or not, this issue can cause a stalemate in security.
9. **Investigative support:** Cloud technology services are difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centres.

III. Study of Security of Cloud Computing in Banking Technology

In order to secure cloud computing infrastructure from potential threats and vulnerabilities at the same time to provide seamless accessibility to various users makes it necessary to put additional security, risk management and business continuity framework in place. With emergence of new technologies, interconnection of various devices, increased use of mobile devices, widespread social networks, proliferation of data and different regulatory norms in various countries makes security framework for cloud architecture even more complex and subject to constant evaluation. Following parameters are too considered in security in Cloud Computing:

1. **Data Privacy:** Data Privacy refers to proper use of customer data provided to Bank & finance organisation for specified purpose. Data collected from customers to meet the business requirements should be accepted by customer and with complete disclosure information being provided to them.
2. **Data Security:** Data security refers to confidentiality, availability and integrity of data. The data security means – it is accessible, used and processed by authorised users only. Data security ensures it is available, reliable and accurate. Data security plan ensures collecting only required information, keeping it safe and destroying any information which is no longer needed.
3. **Information Privacy:** Information privacy refers to the desire of individuals to control or have some influence over data about themselves. Today most communication channels are in digital form through mobile phones and internet, so the personal communication privacy and personal data privacy are merged into information privacy.
4. **Systems Security:** Systems security refers to its ability to protect from external attacks (Deliberate or accidental). Secured systems makes them dependable and available when required, thus makes them reliable. Secured systems when function as expected without failures and any delays helps achieve desired objectives for banking and financial services industry.

3.1 Damage to Systems Security will Lead To

1. **Distributed Denial of services (DDoS)** – Quality of services is degraded or services are unavailable due to failures of multiple infrastructure and network resources. This will lead to unavailability of systems to customers to carry out financial transaction and working staff to perform their operational duties effectively. This will in turn disrupt the normal flow of life and affect economy as a whole. In case of DDoS, the attack may not be detectable as the sources of attack may be from various locations and virtual. This will increase the recovery time required for systems to return to normal business activities.
2. **Corruptions (Tampering) of programs and / or data** – Programs and / or data are modified in unauthorised way. Depending upon the type of program corrupted (financial processing, customer data, storage systems, connectivity devices etc.); the impact will be either financial or operational loss or both. In banking and financial services industry, a small introduction of unacceptable logic in program may not provide the desired outcome from the program and will directly impact both customer and internal working staff. If the website enabling internet banking is updated with informative links and web pages with incorrect scripts, whole internet banking platform may not be available to carry out financial transaction.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 7, Issue 1, July 2021
Impact Factor: 4.819

3. **Disclosure of Confidential Information** – Information may be exposed to people who are not supposed to access it. The amount of data stored in banking and financial services is huge and has variety due to multiple departments.

Any compromise in system security will lead to exposure of risk to assets, loss (monetary or otherwise), vulnerability to future attack or exploitation and loss of control over system. Systems security includes controlling access to physical system and protecting it against harmful network access, code injections and data corruption.

In order to secure system security, it is important to understand the type of threats. Below are common threats to system:

1. **Backdoor:** If someone is able to bypass normal authorization to access system because of poor system configuration, the person may access both personal and financial information. This personal information can be used to open accounts and carry out financial transaction. The nature transaction may look genuine and difficult to detect. Also by the time the transaction is detected as unauthorised the culprits may escape leaving bank with legal and financial implications.
2. **Direct-access attacks:** An unauthorized user gaining physical access to a computer is most likely able to directly copy data from it. They may also compromise security by making operating system modifications, installing software worms, key loggers, covert listening devices or using wireless mice. The unauthorised access may lead to creation of the vulnerabilities in core systems and tampering of the data which will lead to constant data leakages and loss of confidential information (personal or financial) on regular basis.
3. **Eavesdropping:** Eavesdropping is the act of surreptitiously listening to a private conversation, typically between hosts on a network (or two parties). If the communication between host and network which involves disclosing personally identifiable details, account numbers, credit card details etc. is accessed by unauthorised person; the information can be used in future to carry out the financial transaction or steal identify of the person. This will lead to loss of customer information and financial penalties to bank and financial services.
4. **SMS Spoofing:** Through SMS spoofing a user receives a SMS from unknown source asking to provide account details and credentials in order prevent theft or risk of loss of money; through this customer details can be captured during the process and can be used later to steal money from account.
5. **TCP/IP spoofing:** In this type of vulnerability, an email is sent to user (bank's customer) that appears from the genuine source, this technique is powerful as it bypasses the firewall as IP address looks to be external. This method gives access to financial system (server) to external parties which can damage the system as a whole or steal information.
6. **Privilege escalation:** Privilege escalation describes a situation where an attacker with some level of restricted access is able to, without authorization, elevate their privileges or access level. For example, a standard computer user may be able to fool the system into giving them access to restricted data; or even to "become root" and have full unrestricted access to a system.
7. **Phishing:** Through phishing, a customer of the bank may be prompted to enter credentials of the account which can be stored in system and used in future to carry out financial transaction. Due to phishing, bank's customer may lose personal information and financial wealth which will look like authentic for both customer & bank and will go undetected.
8. **Vishing:** Vishing is use of voice and phishing, in which a person pretends to be calling from bank or financial institution in order to access private and financial information from the public. Once, the person gives details (Account number, card information etc.), they are used to perform financial transaction (theft) from bank account which looks genuine and by the person, which leads to financial loss for person. This act can also be termed as Social Engineering.
9. **Cross site scripting (XSS):** XSS is the method to include malicious codes in webpages visited by the user. The data entered by user are later used to create fake identifies; open accounts and perform financial transaction which will cause financial losses to actual customer or person.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 7, Issue 1, July 2021
Impact Factor: 4.819

10. **Pharming:** Pharming is the technique in which the DNS of the bank or financial institution is attacked towards genuine website to provide personal details (and credit / debit card numbers) and account credential to steal money and information of customer.
11. **Insider Threats:** Insider threats are when the employee of the bank or financial institution access and modifies data accidentally which interrupts the everyday operations.
12. **Attack on OTP:** One time password (OTP) is authentication of the user and its credentials while performing the financial transaction. In this type of vulnerability.
13. **Man – In – The - middle (MITM):** Information of the user can be stolen when transaction in process and same information can be used to perform financial transaction (Theft) later.
14. **Man – In – The-Browser (MITB):** Information of the user is captured from website using a fake form and same information is used to create new accounts and financial transaction to steal money.
15. **Man – In – The-PC Attack (MITPC):** In this, weaknesses of the hardware are exploited in order to secure OTP which may be used to perform financial transaction.

3.2 Future Trends in Cloud Computing with Respect to Banking Sector

Companies who view cloud as a journey and not a destination will see more success. This is because simply 'getting to the cloud' doesn't automatically mean you'll see improved performance and spending. Instead, cloud is an repetitive process of optimization and creating security by design to match your company's goals, both now and in the long term. Here's a look at some of the cloud computing trends:

1. **Global Cloud infrastructure market growth at $120B:** The global public cloud infrastructure market will grow 35 percent to $120 billion in 2021. The ability to use the system on the go, whenever and wherever required models to achieve economical service and progress in business is providing the push for organizations to rapidly move forward their digital business change of style plans.
2. **Edge is the next step of Cloud:** Edge is the new cloud, and new edge vendors will trim 5 points from public cloud growth. Over the next few years, buyers will focus their cloud strategies toward the edge to take advantage of all this innovation and become more connected. In future Public clouds will also play a part, it will not be a major player, as the public cloud system is based on massive data centers and tight control of the architecture –which is the exact opposite of what firms are looking to serve customers locally. By adding the network edge into their cloud services, developers have the chance to easily deploy services at the edge without having to worry more operational infrastructures. With merged development and deployment pipelines, cloud developers can move application services and functions from the cloud into network edge locations. This will help create more responsive and dynamic applications. Achieving Superior levels of proper and complete security the network edge distribution is a key challenge for the enterprise and will be enabled by security services at the network edge.
3. **Artificial Intelligence Engineering:** AI projects often are unsuccessful because of lack of good maintenance, less scalability and governance issues, but a good AI engineering strategy will help the performance, scalability, interpretability and reliability of AI models while delivering the full value of AI investments. AI engineering stands on three major pillars: DataOps, ModelOps and DevOps. DevOps deals mainly with high-speed code changes, but AI projects experience dynamic changes in code, models and data, and all must be improved. Organizations must apply DevOps principles across the data pipeline for DataOps and the machine learning (ML) model pipeline for MLOps to reap the benefits of AI engineering. In terms of governance and AI engineering, responsible AI is emerging as an umbrella term for certain aspects of AI implementations to deal with AI risk, trust, transparency, ethics, fairness, interpretability, accountability, safety and compliance.
4. **Joint Cloud Provider Ventures:** There has been increasing trend of partnership between different cloud service providers for providing better service to customers. In June 2019,The Oracle-Microsoft interconnect relationship started is an example of a relationship that could be expanded to take advantage of Oracle's networking and Microsoft's ML capabilities. Rivals Microsoft and Oracle announced in 2019 that they were

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 7, Issue 1, July 2021
Impact Factor: 4.819

linking their clouds to allow joint customers to migrate and run their enterprise application workloads across Microsoft Azure and Oracle Cloud.

5. **Serverless cloud Computing:** Serverless is the next stepfrom service-oriented architecture and micro-services architectures. Serverless was among the top five quickest-growing PaaS cloud services for 2020, this study has been published in the Flexera 2020 State of the Cloud report. Serverless can be considered as actual cloud computing paradigm, and it willnot be an overstatement abouthow much it will impact the cloud is consumed moving ahead. It is such a impressive model, that applications will be designed and developed going forward to work with serverless, rather than serverless being developed to work with the way we currently develop applications. Recently having knowledge of AWS, Azure or GCP capabilities was a key requirement of a cloud application developer. These resources were in high demand. Going forward, this level of detailed knowledge is mooted by serverless, with the serverless interface in cloud becoming the interface developers interact with, not the lower-level interfaces.
6. **Cloud Orchestration:** Cloud platforms will move ahead to create automated cloud orchestration and optimization. The complexity of managing both the quantity and quality of interconnected services across applications and services overwhelms even the savviest of IT organizations. Automated service and performance management will be one of the most important aspects of choosing a cloud provider in future, as most companies will have to manage a hundred or more services from a single cloud provider.
7. **Increase in Cloud Management and Cost Containment Challenges:** For many enterprises, moving workloads to the cloud has greatly improved their operational efficiencies and collaboration, but it has also proven costly. Customers are mostly immature when it comes to presenting their skills sets and are using their cloud infrastructure in an efficient manner compared to how they use their traditional legacy infrastructure. Cloud wastage is a major problem that blocks companies from cloud adoption. Operational inefficiencies are still too great, and customers are not seeing the cost curves being bent down, but staying at a 1:1 ratio. Beyond cloud waste, system platform and management vendors want to be relevant to the rapidly growing cloud computing market, and they understand that managing and operating cloud computing is a new operating paradigm that requires new platforms and tools.
8. **Changing positions of Big Three in Cloud Computing:** There will be reshuffling of the top three public cloud providers in future; China's Alibaba Cloud has replaced Google Cloud to take the No. 3 spot for revenue in the global public cloud infrastructure market. Alibaba is now behind of only No.1 Amazon Web Services and Microsoft Azure. Alibaba's cloud computing revenue grew 59 percent year-over-year to $2.19 billion for the quarter that ended Sept. 30. Alibaba's cloud computing is driven by the acceleration in digitalization across industries and businesses of all sizes in China. Revenue from customers in the internet, finance and retail industries was the primary growth drivers. Google Cloud's revenue which includes sales from Google Cloud Platform (GCP), Google Workspace (formerly G Suite) productivity tools and other enterprise cloud services – increased to $3.44 billion, compared to $2.38 billion in the same quarter last year.
9. **Increasing requirement of Data Privacy And Cloud Migration:** The combination of the coronavirus pandemic and an increase in cloud infrastructure will create the "perfect storm" for data governance and compliance from 2021 Organizations will move to initiate projects to make sure secure data migration to the cloud which means encryption of all data that is needed to be submitted to the enterprise data governance team before their IT team or their data teams are allowed to move data from on-prem system to the cloud. From 2021, data governance will become an even more topic of considerations for Chief Information Officers (CIOs), chief information security officers (CISOs), and Chief data officers (CDOs) to ensure responsible use and availability of cloud data. In future, Regulatory legislation around the world will move toward increased control of personally identifiable information (PII) data to safeguard consumer privacy. Many countries are increasingly following the steps of the European Union's General Data Protection Regulation (GDPR).Standalone data security and governance tools finally will become an integral part of mission-critical business processes

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 7, Issue 1, July 2021
Impact Factor: 4.819

10. **SASE Adoption& its Growth:** "Secure Access Service Edge (SASE) will be more favourable to gain adoption as organizations are moving ahead of the quick response measures they applied during 2020 because of Global Pandemic. From 2021 there will be massive and unexpected increase in remote worker connectivity. SASE is pronounced as "sassy" and it is primarily delivered as a cloud-based service, SASE is a network architecture that combines software-defined WAN capabilities and cloud-native network security services including zero-trust network access, secure web gateways, cloud access security brokers and firewalls as a service. Many IT networking groups unluckily found the stress, strain and limits of their remote access VPN concentrators and, even after overcoming or addressing those breaking points, they next coped with emerging issues in their bandwidth constraints, lack of network segmentation, weakness in endpoint security solutions and myriad untrusted devices connecting to sensitive corporate systems. Wise IT groups will budget and start planning for a more converged and integrated cloud-based approach to remote device, workforce and distributed security technology.
11. **Limitations in Usage of Data Warehousing:** A Data Warehousing (DW) is process for collecting and managing data from varied sources to provide meaningful business insights. A Data warehouse is typically used to connect and analyze business data from heterogeneous sources. The data warehouse is the core of the BI system which is built for data analysis and reporting. It is a blend of technologies and components which aids the strategic use of data. It is electronic storage of a large amount of information by a business which is designed for query and analysis instead of transaction processing. It is a process of transforming data into information and making it available to users in a timely manner to make a difference.

The Future of Data Warehousing

1. Change in Regulatory constrains may limit the ability to combine source of disparate data. These disparate sources may include unstructured data which is difficult to store.
2. As the size of the databases grows, the estimates of what constitutes a very large database continue to grow. It is complex to build and run data warehouse systems which are always increasing in size. The hardware and software resources are available today do not allow to keep a large amount of data online.
3. Multimedia data cannot be easily manipulated as text data, whereas textual information can be retrieved by the relational software available today. This could be a research subject.
12. **Growth in use of Containers:** Containers offer a seamless development process due to its capacity to provide portability between multiple platforms and clouds, efficiency, and delivering higher utilization of resources. The development and deployment process becomes a matter of minutes due to their effortless working with microservice-based architecture. The combination of containers with microservice enables a product to spin rapidly and get to the market quickly. DevOps is always about better software delivery and container orchestration has contributed to this goal. Overall, containerization helps in staying ahead of the curve and serves the ever-changing demands and standards of the market. Containers use kubernates which is an open-source, portable, and extensive platform, Kubernetes or k8 is used to manage containerized workloads and services that facilitate automation for application deployment, scaling, and management. Kubernates has following features like Self-healing, Load balancing, Storage orchestration, Automatic bin packing, Sensitive information and configuration management. Artificial Intelligence Operations–AI Operations, an application of artificial intelligence (AI), uses big data, analytics, and machine learning capabilities to improvise the IT operations and ease the challenges of modern day IT infrastructure.

3.3 Benefits of AI

1. Collection of the ever – increasing data.
2. Aggregating the collected data.
3. Intelligent clustering of data to identify events and patterns that may cause issues.
4. Identifying the root causes of these issues.
5. Immediate alerts about the causes and enables rapid response from the IT team for remediation.
6. Reduction in slowdowns and outages efficiently and intelligently.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 7, Issue 1, July 2021
Impact Factor: 4.819

IV. CONCLUSION

In this article we have learned about the brief analysis of cloud computing, its types& impact on Banking sector. Along with that we have learned about security of Cloud computing & its future trends. Government initiative of Digital India has been a driving force for indian banks to adopt to cloud computing. Current scenarios of pandemic have given a major boost to Cloud computing to make a substantial progress. This rapid progress in Cloud computing has raised many questions regarding its security; we hope this article has answered many of those questions. This article also has focused on future trend of cloud computing which will give a better idea of what's next in the field of cloud computing.

REFERENCES

[1]. The-Future-of-Cloud-Computing-for-Banking-Industry – by Meshal Alabdulwahab
[2]. Implementation of Cloud Computing on Web Application – by Liladhar R. Rewatkar & Ujwal A. Lanjewar
[3]. The impact of Cloud Computing in the banking industry resources – by Najla Niazmand
[4]. Data Privacy and System Security for Banking and Financial Services Industry based on Cloud Computing Infrastructure– by Abhishek Mahalle
[5]. https://www.guru99.com/data-warehousing.html
[6]. https://www.fortunesoftit.com/top-7-containerization-trends-for-2021/