IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

Effects of Cloud Computing on the Banking Industry, as well as Future Trends

Ritik Shekhar Kamerkar
Student, Master of Computer Application
Late Bhausaheb Hiray S. S. Trust's Hiray Institute of Computer Application, Mumbai, India

Abstract: *The Digital India project of the Indian government has pushed banks and other financial institutions to use cloud computing. Because of this, cloud computing has experienced rapid expansion across all industries. Many enterprises in the public and private sectors have begun to use cloud computing as their preferred method for storing and analysing data that can be accessed from any location at any time. The cost of managing both technical and physical infrastructure has decreased as a result of cloud computing. After adopting cloud computing as a means of storing data and analysing security frameworks while retaining privacy, the banking sector in particular has experienced significant growth. With the introduction of cloud computing, the banking services sector is still subject to stringent regulatory and compliance frameworks to uphold data privacy and system security. We will study about cloud computing and how it affects the banking industry in this document. Along with that, we'll learn about some potential cloud computing trends for the banking industry.*

Keywords: Finance, BLDC, ZETA, MPPT, PV, Cloud, Security, Banking

I. INTRODUCTION

1.1 What is Cloud Computing?

The phrase "cloud computing" and the word "cloud" are both metaphors for the internet. The term "cloud" is derived from the ancient cloud symbol, which was frequently used in flow charts to depict the internet. Application, data, network, storage, and server resources for information systems are made accessible and usable through the utilisation of the cloud.

You must be present where your storage device is for a typical setup. Accessing the data from anywhere at any time is made simpler by cloud computing. The cloud eliminates the requirement that you be present in the same physical space as the gear used to store your data.

A system that enables easy on-demand network access to a pool of configurable computing resources (such as networks, servers, storage, applications, and services) that can be quickly provisioned and released with little management work or service provider involvement is known as cloud computing.

1.2 Various Cloud Types

Depending on the demands of the customer, numerous types of clouds may be considered for use.

- **Public cloud**-Anyone with an internet connection and access to the cloud space can use a public cloud.
- **Private cloud**-a private cloud is created for a certain group or organisation and only allows members of that group to access it.
- **Community cloud**-a community cloud is shared by two or more businesses with comparable cloud computing needs.
- **Hybrid cloud**-A hybrid cloud is simply the merger of at least two clouds, where the clouds combined are a mix of community, private, and public clouds.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

1.3 Different Cloud Service Provider

Depending on the kind of provider selected, each cloud service offers distinct features that provide clients control over the cloud. Three different categories of cloud service providers exist:

- **Software as a Service (SaaS)** - A SaaS provider enables access to resources and applications for the client. Software as a service eliminates the need for a physical copy of the programme to be installed on your devices. By accessing it over the cloud, SaaS also makes it simpler to have the same software on all of your devices at once. Client has the least control over the cloud under a SaaS arrangement.
- **Platform as a Service (PaaS)** - This technology advances the software as a service model. A PaaS provider offers Client access to the elements they need to create and manage web applications.
- **Infrastructure as a Service(IaaS)**-As implied by the name, an IaaS agreement focuses largely on the infrastructure used for computing. The subscriber totally outsources the storage and resources, including the hardware and software, they require under an IaaS arrangement.

1.4 Different Forms of Cloud Operating Models

A suitable cloud operating model that offers a combination of suitable assets and resources is necessary for a suitable cloud service model. The following sorts of cloud operating models are possible:

- **Staff Augmentation** - Organisations may increase their cloud knowledge by hiring qualified cloud specialists from cloud service providers. With this operational paradigm, enterprises may select the optimum resource for any given need.
- **Virtual captives** -Virtual captives have specialised staff or facilities to support cloud operations and handle demand.
- **Outsourcing vendors** -Using third-party suppliers to manage cloud operations - This strategy makes use of employees who work for organisations outside of their own. The strategy combines investments and resources to support cloud services.

II. CLOUD COMPUTING'S IMPACT ON THE BANKING SECTOR

Banks are moving to cloud computing for a variety of reasons. The following list of important causes is described. Since data may be stored and accessed immediately over the internet & virtual service, less hardware & storage facility is required. Utilising software, computers, and other devices as a utility over a shared network, cloud computing provides computational power as a virtual service.

- **Lower costs:** One key benefit of cloud computing is that there is no need for on-site hardware storage. Banks can save their IT costs by not using physical hardware. Banks may simply purchase a subscription from a cloud service provider and utilise it, eliminating the need for physical infrastructure and IT staff.
- **Streamlining business processes:**Clients may access easily available data anytime they need it thanks to cloud computing and storage. A correct resource management is made possible by a much decreased technological workload between the processor and the server.
- **Ease of use:**There are no concerns about resource management or other issues related to infrastructure setup and management while using cloud computing, which makes it easy to set up all the services.
- **Reliability:** Given that the service providers are professionals at managing the infrastructure, network and data access are guaranteed to be maintained in a reliable manner.
- **Flexibility:** Clients have the option to "outsource" some components of the infrastructure while yet keeping some private data on-site.
- **Privacy and Security:** Even if access-control and encryption software is available, cloud computing enables customers to add additional capacity, more services, and seamless software patching.
- **Data segregation:** Data segregation is important since the cloud is a shared environment where information may be exchanged. The risk of data loss exists. The service provider must guarantee that encryption is accessible at all times and that the encryption patterns were created and tested by qualified experts.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

- **Recovery:** When an issue arises and a failure results, data recovery is crucial. The key concern that emerges is whether or not the cloud provider can fully recover the data. If this problem persists, security may come to a standstill.
- **Investigative support:** Cloud technology services are challenging to look into since logs and data for various clients may be co-located and/or distributed over a constantly shifting array of hosts and data centres.
- **Improved Customer Experience:** Banks may provide their consumers improved digital experiences thanks to cloud-based technology. Banks are swiftly able to create and implement cutting-edge online and mobile banking programmes, providing consumers with practical self-service alternatives, immediate access to account information, and individualised services.
- **Regulatory Compliance:** Cloud service providers frequently follow security standards and industry rules, which can help banks more effectively satisfy their regulatory requirements. Banks may better navigate complicated regulatory environments by utilising the compliance knowledge of cloud providers.

III. STUDY OF SECURITY OF CLOUD COMPUTING IN BANKING TECHNOLOGY

Additional security, risk management, and business continuity framework must be put in place in order to protect cloud computing infrastructure from potential attacks and vulnerabilities while ensuring seamless accessibility to varied users. The security framework for cloud architecture is becoming increasingly complex and is subject to ongoing evaluation due to the emergence of new technologies, the interconnection of various devices, the rise in mobile device use, the widespread use of social networks, the proliferation of data, and different regulatory norms in various countries. The following factors are also taken into account for security in cloud computing:

- **Data Privacy:** Data Privacy refers to the appropriate use of client information submitted to banks and financial organisations for a defined purpose. Customers should consent to the collection of their data for commercial purposes and get full disclosure of any such data collection.
- **Data Security:** The confidentiality, accessibility, and integrity of data are all covered under data security. Data security ensures that only authorised people may access, utilise, and manipulate the data. Data security guarantees its accessibility, dependability, and accuracy. Data security plans guarantee that only the information that is necessary is collected, that it is protected, and that any information that is no longer required is destroyed.
- **Information Privacy:** The desire of people to have some control or influence over information about themselves is referred to as information privacy. The majority of communication routes today are digital, including mobile devices and the internet, therefore information privacy includes both private communication and private data.
- **Systems Security:** The capacity of a system to fend off outside threats, whether intentional or unintentional, is referred to as systems security. Systems that are secure are more trustworthy and readily accessible when needed. Secured systems that perform as intended without issues or delays aid the banking and financial services sector in achieving its goals.

Systems Security Damage Will Lead To

- **Distributed Denial of services (DDoS)** – Services are unavailable or of reduced quality as a result of the breakdown of several infrastructure and network resources. Customers won't be able to conduct financial transactions on these systems, and employees won't be able to efficiently carry out their operational obligations. This will therefore cause a disruption in daily life and have an impact on the economy as a whole. When a DDoS assault occurs, it's possible that it won't be seen because the attack's sources might be both physical and virtual. As a result, it will take longer for systems to recover and resume regular operations.
- **Corruptions (Tampering) of programs and / or data** – Unauthorised changes are made to programmes and/or data. Financial or operational loss, or perhaps both, depending on the type of corrupted programme (financial processing, customer data, storage systems, communication devices, etc.). In the banking and financial services sector, even a tiny amount of improper logic introduced into a programme might prevent it from producing the desired results and have a negative influence on both internal working people and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

customers. The entire online banking platform could not be accessible to conduct financial transactions if the website supporting internet banking is updated with useful links and web pages with improper scripts.

- **Disclosure of Confidential Information** – Confidential information may be disclosed to individuals who are not authorised to see it. Due to the several departments, the amount of data stored in banking and financial services is enormous and diverse.

Any breach in system security exposes assets to risk, results in a loss (financial or otherwise), makes the system vulnerable to future assault or exploitation, and loses control. Controlling physical system access and defending it from damaging network access, code injections, and data manipulation are all part of systems security.

Understanding the different risks is crucial for protecting system security. The following list of typical system risks:

- **Backdoor:** Someone may access both personal and financial information if they are able to go around the system's standard authorisation process due to bad system design. It is possible to create accounts and conduct financial transactions using this personal information. The nature transaction could appear real and be hard to spot. Additionally, the perpetrators may have escaped by the time the illegal transaction is discovered, leaving the bank vulnerable to legal and financial consequences.
- **Direct-access attacks:** It is most likely possible for an unauthorised person to physically enter a computer and copy data from it directly. They could also alter the operating system, put in software worms, keyloggers, hidden listening devices, or use wireless mouse to breach security. Unauthorised access may result in the development of vulnerabilities in crucial systems and data manipulation, which will frequently cause data leaks and the loss of private information (personal or financial).
- **Eavesdropping:** The act of secretly listening to a private discussion, usually between hosts on a network (or two parties), is known as eavesdropping. If an unauthorised individual intercepts communication between the host and the network during which personally identifiable information, such as account numbers, credit card numbers, and other data are disclosed, the information may later be used to commit fraud or steal the victim's identity. Loss of consumer information and financial fines for banks and financial services will result from this.
- **SMS Spoofing:** Through SMS spoofing, a user receives an SMS from an unexpected source requesting account information and login credentials in order to prevent theft or the risk of losing money. Through this procedure, client information can be acquired and then used to steal money from the user's account.
- **TCP/IP spoofing:** In this sort of vulnerability, a user (a bank client) is sent an email that appears to be from a reliable source. This approach is effective since it gets past the firewall because the IP address appears to be external. Through this strategy, other parties are given access to the financial system's server, giving them the opportunity to steal information or harm the system as a whole.
- **Privilege escalation:** Privilege escalation refers to a circumstance in which an attacker with a limited amount of access can escalate their privileges or access level without being given permission. As an illustration, a regular computer user may be able to trick the system into granting them access to protected data or even "become root" and have complete, unlimited control over a system.
- **Phishing:** Through phishing, a bank customer may be asked to submit account information that will be saved in the system and utilised later to conduct financial transactions. Due to phishing, bank customers risk losing private information and money, which will appear genuine to the consumer and the bank and will go unnoticed.
- **Vishing:** Vishing is the use of voice and phishing, in which a person poses as a bank or financial organisation to phone in order to gain personal and financial information from the general public. Once the victim provides their information (account number, card number, etc.), they are then utilised to conduct financial transactions (theft from bank accounts) that appear legitimate and cause the person to suffer financial loss. This behaviour is also known as social engineering.
- **Cross site scripting (XSS):** Cross-site scripting (XSS) is a technique for inserting malicious code into user-visited webpages. The information supplied by the user is afterwards utilised to construct fictitious identities, open accounts, and carry out financial transactions that result in losses for the real client or person.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

- **Pharming:** Pharming is a technique where a bank or other financial institution's DNS is attacked against a legitimate website to get personal information (such as credit or debit card numbers) and account credentials in order to steal money and client information.
- **Insider Threats:** An insider threat occurs when a bank or financial institution employee unintentionally accesses and edits data, disrupting routine business.
- **Attack on OTP:** One time passwords (OTPs) are used to authenticate users and their credentials while carrying out financial transactions. In this kind of exposure.
- **Man-In-The-middle (MITM):** When a transaction is in progress, user information can be taken and later utilised to commit a financial transaction (theft)..
- **Man-In-The-Browser (MITB):** Using a false form, information about the user is taken from a website and used to open new accounts and conduct financial transactions to steal money.
- **Man-In-The-PC Attack (MITPC):** This involves taking advantage of hardware flaws to secure an OTP that might be used to conduct financial transactions.

Cloud Computing Future Trends with Regard to the Banking Sector

Businesses that perceive the cloud as a journey rather than a final destination will be more successful. This is due to the fact that merely "going to the cloud" does not guarantee superior expenditure and performance. Instead, the cloud is an ongoing process of security by design and optimisation to meet your business's short- and long-term objectives. Cloud computing is anticipated to continue playing a big role in the banking sector in the next years, allowing financial organisations to improve their operations, enhance client experiences, and spur innovation. Following are a few anticipated cloud computing trends for the banking industry:

- **Hybrid Cloud Adoption:** To strike the proper balance between security, compliance, and cost-effectiveness, banks are expected to embrace hybrid cloud models, which integrate public and private clouds. Banks may utilise the scalability and flexibility of public clouds for non-sensitive data and apps while maintaining crucial and private data in private clouds or on-premises using hybrid cloud configurations.
- **Increased Data Security:** Since cyberattacks and data breaches are still important issues for the banking sector, cloud service providers will make significant investments to strengthen security protocols. Cloud computing systems with robust encryption, access restrictions, threat detection, and data loss prevention features will be given priority by banks. on addition, they will use technologies like confidential computing to safeguard private information while it is handled on the cloud.
- **Artificial Intelligence Engineering:** 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 projects frequently fail due to poor maintenance, limited scalability, and governance issues. DataOps, ModelOps, and DevOps are the three main pillars that support AI engineering. While AI projects face dynamic changes in code, models, and data, all of which must be improved, DevOps mostly works with high-speed code updates. To benefit from AI engineering, organisations must use DevOps concepts throughout the data pipeline for DataOps and the machine learning (ML) model pipeline for MLOps.In terms of governance and AI engineering, "responsible AI" is becoming a catch-all word for certain AI implementations that deal with risk, transparency, ethics, fairness, interpretability, accountability, safety, and compliance.
- **Open Banking and APIs:** Cloud computing will help open banking efforts, which promote cooperation and data exchange between financial institutions and outside sources. Banks will be able to safely expose their APIs through cloud-based platforms, fostering ecosystems where clients may access a variety of financial services and products from many suppliers via a single interface. The scalability and agility of the cloud will make it easier to integrate different apps and services in an open banking setting.
- **Serverless cloud Computing:** The next step from service-oriented architecture and micro-services architectures is serverless cloud computing. According to a survey that was released in the Flexera 2020 State of the Cloud report, serverless was among the top five PaaS cloud services with the fastest expanding user bases in 2020. It is not an overstatement to say that serverless computing is a true cloud computing paradigm and will have a significant future effect on how cloud computing is used. Because of how remarkable this

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

paradigm is, apps will be created in the future so that they can operate with serverless rather than serverless being created so that it can work with how we create applications now. Recently, one of the most important qualifications for a cloud application developer was familiarity with AWS, Azure, or GCP capabilities. There was a big need for these materials.Serverless is proposing that in the future developers communicate with the serverless interface rather than lower-level interfaces, which would need this degree of in-depth understanding.

- **Regulatory Compliance:** Strict regulatory frameworks are in place for the banking industry, and cloud computing may help with compliance. Cloud service providers will provide tools and services including data encryption, audit trails, and compliance management platforms that are particularly made to assist regulatory compliance. Banks will make use of these capabilities to make sure they adhere to local and federal financial rules as well as data protection and privacy laws, such as the GDPR.
- **Growing Cloud Management and Cost Containment Challenges:** Moving workloads to the cloud has significantly increased operational efficiency and cooperation for many companies, but it has also proven to be expensive. When it comes to communicating their skill sets, customers tend to be immature. However, they use cloud infrastructure more effectively than they use traditional legacy technology. The main issue preventing businesses from adopting cloud computing is cloud waste. Customers do not see the cost curves as being bent down but rather as remaining at a 1:1 ratio because operational inefficiencies are still too significant. Beyond cloud waste, system platform and management suppliers want to stay relevant in the quickly expanding cloud computing industry. They are aware that managing and running cloud computing requires new platforms and tools since it is a new operating paradigm.
- **Edge Computing for Branch Transformation:** Edge computing will be essential as banks continue to modernise their branch networks. Edge computing reduces latency and enables real-time processing by bringing computation and data storage closer to the source of data production. To support services like personalised offers, rapid loan approvals, and enhanced client interactions, banks can set up edge computing equipment in their branches. The administration and orchestration of edge devices will be made easier by the use of cloud platforms, which will also make it possible for a seamless interaction with central banking systems.
- **Increasing requirement of Data Privacy And Cloud Migration:** The coronavirus pandemic plus an expansion in cloud infrastructure will produce the "perfect storm" for data governance and compliance starting in 2021. 9. Increasing Requirements for Data Privacy and Cloud Migration In order to ensure safe data migration to the cloud, organisations will move to launch projects. This entails encrypting all data that must be presented to the corporate data governance team before their IT team or their data teams are permitted to migrate data from on-prem system to the cloud. To guarantee responsible usage and accessibility of cloud data, chief data officers (CDOs), chief information security officers (CISOs), and chief information officers (CIOs) will all be considering data governance more and more starting in 2021.In order to protect consumer privacy, regulatory regulation will shift towards greater management of personally identifiable information (PII) data in the future. The General Data Protection Regulation (GDPR) of the European Union is being progressively adopted by several nations. Finally, mission-critical business operations will fully integrate standalone data security and governance solutions.
- **Disaster Recovery and Business Continuity:** Cloud computing provides banks with strong disaster recovery and business continuity capabilities. To ensure data redundancy and prompt recovery in the case of system failures, natural catastrophes, or cyberattacks, banks will use cloud-based backup and replication services. Banks may disperse workloads across many locations using cloud environments, which also offer high availability and resilience.
- **Restrictions on Data Warehousing Use:**A data warehousing (DW) process is used to gather and manage data from many sources in order to provide insightful business information. Business data from many sources is often connected and analysed using a data warehouse. The central component of the BI system, which is designed for data analysis and reporting, is the data warehouse. The combination of several technologies and elements facilitates the strategic use of data. Large amounts of data are electronically stored by a company and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

are intended for analysis and inquiry rather than transaction processing. It is a process of converting data into information and promptly making it accessible to people so that it might have an impact.

IV. FUTURE PROSPECTS FOR DATA WAREHOUSING

- The capacity to merge sources of different data may be constrained by changes in regulatory constraints. Unstructured data from these many sources, which is difficult to store, may be present.
- As databases get bigger, estimations of what counts as a very large database also get bigger. Building and maintaining ever-growing data warehouse systems is difficult. A significant quantity of data cannot be kept online with the technology and software resources that are now available.
- Textual information may be accessed by relational software, but multimedia data cannot be as simply altered as text. This may be a topic for investigation.

Advantages of AI

- Gathering of the ever-growing data.
- Combining the data gathered.
- Using intelligent data clustering to find occurrences and trends that could be problematic.
- Determining the underlying reasons of these problems.
- Immediate warnings of the issues and the ability for the IT staff to take corrective action quickly.
- Effective and intelligent slowness and outage reduction.

IV. METHODOLOGY

Proposed data security model in cloud computing:

The model made use of a three-layer system structure, with each floor carrying out a specific task to guarantee the privacy of the cloud tiers' data.

The first layer, which is in charge of user authentication, nearly always uses two factors, however free cloud providers like eyeos, cloudo, and freezoha just require one.

The second layer is in charge of encrypting user data and employing one symmetric encryption technique to safeguard users' privacy in a certain manner. Allow user protection as well.

The user data for quick recovery is the third layer. Depending on how quickly the encryption is brokenWe enhance the cloud computing data security model. We add software to the cloud service provider. Two-factor authentication is used in this software's implementation. This freeware evaluates eight modes of modem encryption. This comparison used statistical tests to determine which security methods were more effective. This programmeutilises a cloud-based architecture and a quicker, higher-security algorithm. Therefore, we suggested the appropriate, higher-security encryption technique for the cloud provider's platform. Finally, by this examination, we guarantee user data security and speedier data retrieval.

We also create software for cloud users. With this programme, users may select from eight different encryption techniques to protect their data. This programme offers suggestions to the cloud customer on the fastest, safest, or most secure algorithm for their cloud infrastructure.Some issues are resolved by suggested software. This programme uses two-way authentications to enable robust API access control. This app uses the best security algorithm to encrypt and safeguard data. IAAS uses Amazon EC2 as a case study for this software's investigation of data protection. Using NIST statistical checks, this programme assures that the protection method is the highest security algorithm to satisfy the user. quicker retrieval is guaranteed by this programme when employing a quicker encryption/decryption technique.As can be seen, the Amazon EC2 provider must employ AES to guarantee the highest level of data security.

The first recommendation is for users of the Amazon EC2 cloud who are more concerned with algorithm performance than they are with data security. You must employ blowfish, DES, or AES, which encrypt data more quickly and in less time than other methods.

The second piece of advise is for customers of the Amazon EC2 cloud who are looking for improved data protection. The best security algorithm, AES, must be used.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

The third and final piece of advise is that AES, which is the most secure and requires the least amount of time to encrypt, is appropriate for Amazon EC2.

V. CONCLUSION

In this post, we learnt about a quick examination of cloud computing, its variations, and its effects on the banking industry. Additionally, we have learnt about the security of cloud computing and its potential future developments. The government's Digital India project has pushed Indian banks to adopt cloud computing. Pandemic situations in the present have significantly accelerated cloud computing's development. We believe this essay has addressed many of the security-related problems that have been generated by the fast advancement of cloud computing. To offer readers a clearer picture of what's to come in the field of cloud computing, this article also concentrated on future trends in cloud computing.

In conclusion, cloud computing has completely changed the banking industry and offers enormous advantages in terms of innovation, client experience, and operational efficiency. But maintaining the security and privacy of client data continues to be of the utmost importance. The banking sector may fully utilise cloud computing and spur more developments in the digital era by resolving security issues and embracing future trends.

REFERENCES

[1] The-Future-of-Cloud-Computing-for-Banking-Industry–byMeshalAlabdulwahab
[2] Cloud Computing Research and Development Trend–byShuai Zhang; Shufen Zhang; Xuebin Chen; Xiuzhen Huo
[3] Rittinghouse, J. W., & Ransome, J. F. (2016). Cloud computing: Implementation, management, and security. CRC Press.
[4] The impact of Cloud Computing in the banking industry resources– byNajlaNiazmand
[5] Loebbecke, C., & Picot, A. (2015). Reflections on societal and business model transformation arising from digitization and big data analytics: A research agenda. Journal of Strategic Information Systems, 24(3), 149-157.
[6] Enhanced data security model for cloud computing – by EmanMeslhy
[7] https://www.guru99.com/data-warehousing.html
[8] https://www.fortunesoftit.com/top-7-containerization-trends-for-2021/