

Share — copy and redistribute the material in any medium or format for any purpose, even commercially. Adapt — remix, transform, and build upon the material for any purpose, even commercially. The licensor cannot revoke these freedoms as long as you follow the license terms. Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made . You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use. ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original. No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits. You do not have to comply with the license permits of the material in the public domain or where your use is permitted by an applicable exception or limitation. No warranties are given. The license for elements of the material in the public domain or where your use is permitted by an applicable exception or limitation. necessary for your intended use. For example, other rights such as publicity, privacy, or moral rights may limit how you use the material. In 2023, the worldwide cloud computing market achieved a valuation of USD 579.58 billion, and it is anticipated to expand at a steady pace of 13.5% between 2023 and 2033, ultimately reaching an impressive value of USD 2,062.26 billion by 2033. With the growing realization of the immense benefits of using public cloud computing service providers catering to a huge demand for various remote facilities. What are the Different Market Dynamics Propelling the Global Cloud Computing Market? Given the immense advantages of integrating cloud-based servers for small businesses for increasing their customer base. Cloud computing architecture enables streamlined business operations and quick adaptation to the market. Transitioning to a cloud-based infrastructure fuels global demand for cloud computing, improving efficiency and agility. Integration of cloud computing systems streamlines technology use and drives behavioral changes among workers. based servers for small businesses. Introduction of modern digital technologies like big data analytics and AI creates high demand for scalability, flexibility, and cost-efficiency in IT infrastructure. Rising need for data storage, processing, and analysis capabilities. Emergence of edge computing and hybrid cloud solutions. Growing reliance on Software-as-a-Service (SaaS) and Infrastructure-as-a-Service (IaaS) models. Enhanced cybersecurity measures and data protection in cloud environments. What are the Key Obstacles Impeding the Progress of Market Participants? The following are likely to prove as challenges that participants are confronted with: Security of data stored on open-source security storage platforms is a key concern for cloud computing providers. External vulnerabilities pose risks to the stored data, potentially hindering market growth. Regulations related to data privacy in cross-border security storage networks are a significant limitation for the global market for cloud computing. Compliance with data privacy regulations beyond national borders presents challenges to wide market acceptance. Dominance of leading cloud market acceptance of industry giants like Google and Microsoft can be highly challenging for new cloud computing adds to the difficulties faced by new companies in their initial operations. Attributes Details Cloud Computing Market Value (2023) USD 579.58 billion Cloud Computing Market Value (2033) USD 2,062.26 billion Cloud Computing Market Growth Rate (2023 to 2033) 13.5 %. Explore FMI! Book a free demo What is Fueling the Cloud Computing Market? Improving digital literacy around the world and the rapid adoption of digital applications for enhancing the user experience has compelled many service-based companies to blend in several features in their production systems. This need for combining many different digital features is promoting the use of cloud computing providers. The market is also getting high traction in the form of long-term subscriptions to personal cloud computing services these days decreased the cost of production by reducing the requirement of hiring on-site employees. This stands as a prominent point for the high popularity of cloud computing services in the global market. Segmentation Analysis What is Contributing to the Leading Position of Software as a Service (SaaS) Sub-segment on the Basis of Service Type? As per FMI study, the Software as a Service (SaaS) sub-segment led the market, holding a value share of 52.7% globally in 2022. The rising enterprise demand is expected to accelerate the growth of the Software as a Service (SaaS) sector, driven by its simple deployment and low maintenance requirements. Its subscription-based model provides cost efficiencies by eliminating upfront infrastructure investments. SaaS sub segment also simplifies deployment and updates, relieving organizations of maintenance tasks. By leveraging SaaS, organizations of maintenance tasks. By leveraging SaaS sub segment also simplifies deployment and updates their core competencies and strategic goals. resources and efforts toward their primary areas of expertise. This results in improved productivity and efficiency. Which Deployment Model Segment of the Cloud computing Market Holds a Substantial Share? The applicability of cloud computing networks has covered a lot of areas in any economy. Most end users prefer the public cloud segment owing to its great affordability and easy availability of users. In the coming years, this segment is expected to continue its dominance over the cloud deployment segment has also been analyzed to be gaining momentum with the introduction of some popular personal cloud computing products in the market. Individual customers mostly go for the best cloud backup for PC, which is anticipated to create some attractive opportunities for the market players. What is the Performance of the Cloud Computing Industry in Different Geographical Regions? Regions CAGR (2023 to 2033) The United Kingdom (UK) 12.5% China 13.7% India 13.1% What Elements Bolster North America's Unrivaled Supremacy in the Cloud Computing, North America holds the significant share by contributing about 34.6% of the revenue as per the 2022 records. Due to the presence of most of the leading companies such as Google computing, Amazon cloud services, Microsoft edge computing, and others, the market in the United States of America boasts a thriving business ecosystem, with several enterprises embracing cloud computing solutions. The region's mature market, entrepreneurial culture, and technological adoption contribute to its supremacy. The regulatory environment in North America, characterized by clear data protection and privacy laws, fosters trust and confidence among businesses and consumers, facilitating the widespread adoption of cloud computing services. What are the Prominent Drivers Fueling the Growth of the Cloud Computing Industry in the Asia Pacific Region? During the forecast time period, the growth of Asia Pacific cloud computing market share be high than in any other geographic region. The evolution of a robust IT sector and the emergence of new cloud market shareholders have provided the necessary impetus for a significantly growing market in the region. In accordance with the FMI research, the market for cloud computing in China is estimated to account for a significant portion of market share, advancing at a CAGR of 13.7% and India at a rate of 13.1% from 2023 to 2033. Asia Pacific region is witnessing a significant digital transformation across various industries. Organizations are adopting cloud computing to modernize their operations, enhance agility, and drive innovation. What is the Prevailing Landscape and Market Position of Cloud Computing providers in Europe and Latin America has also surged considerably in the past decade. With the growing demand for cloud computing services, the market is estimated to experience positive growth in these regions as well. Europe has emerged as a significant player in the global cloud computing arena, witnessing substantial growth and adoption across various industries and sectors. Moreover, key market players, both regional and global, have established a strong presence in Europe, offering a wide range of cloud services and solutions to cater to diverse customer needs. This competitive market environment fosters innovation, drives technological advancements, and fuels the continuous evolution of cloud computing in the region. The demand for scalable and cost-effective IT infrastructure solutions is fostering the cloud computing market size in the United Kingdom, providing impetus to its growth rate of 12.5% from 2023 to 2033. What is the Competitive Scenario for the Cloud Computing Industry? features in their cloud computing services as per the changing working models and demands from users. The giant cloud companies are also spending on establishing data storage networks and speed up data transfer. This constant evaluation process adopted by cloud computing agencies has improved the performance of public cloud computing platforms over the years. It is further anticipated to increase the number of cloud computing Market? Embracing Multi-cloud Approaches Embraced by Players in the Cloud Computing Market? multiple cloud service providers to achieve enhanced performance, flexibility, and redundancy. Offering Vertical-specific Solutions: Players focus on developing industry-specific cloud solutions tailored to the unique needs and requirements of different sectors, such as healthcare, finance, or retail. Prioritizing Security and Compliance: Players invest in robust security measures, data encryption, and compliance certifications to address concerns related to data
protection and regulatory requirements. Enhancing Data Analytics Capabilities: Players integrate advanced analytics and make data driven decisions. What are the Recent Developments in the Field of Cloud Computing Industry? The leading telecommunication company in the United States of America named, AT&T, signed an agreement with Microsoft Inc. in July 2021 from getting into a partnership. This partnership is anticipated to avail the Microsoft cloud computing platform for running the core parts of the 5G wireless network provided by AT&T. In September 2021, Telefonica España and Oracle collaborated on the development of new communication services for consumers as well as telecom businesses over the Oracle Exadata Cloud. Key Players Operating in the Cloud Computing Market AWS Microsoft IBM Salesforce Google Oracle SAP Alibaba Cloud Adobe Workday The market is valued at USD 579.5 billion in 2023. The market players. Technological advancements to boost the market prospects. The software-as-a-serice segment is likely to remain preferred through 2033. Question: Which statement describes a characteristic of cloud computing? A business can connect directly to the Internet without the use of an ISP. Applications can be accessed over the Internet through existing electrical wiring. Investment in new infrastructure is required in order to access the cloud. Explanation: Cloud computing allows users to access resources through subscription-based or pay-per-use services, in real time, using nothing more than a web browser. Exam with this question: CCNA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam with this question: IT Essentials (ITE v7) Chapter 9 Exam Answers Exam with this question: CVA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam with this question: IT Essentials (Version 1.0) - Modules 13 - 16: Home Network Basics Pre-Test Exam With this question: CVA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam with this question: IT Essentials (Version 2) - Modules 13 - 16: Home Network Basics Pre-Test Exam Answers Exam With this question: CVA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam With this question: IT Essentials (Version 2) - Modules 13 - 16: Home Network Basics Pre-Test Exam Answers Exam With this question: CVA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam With this question: CVA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam With this question: CVA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam With this question: CVA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam With this question: CVA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam With this question: CVA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam With this question: CVA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam With this question: CVA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam With this question: CVA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam With this question: CVA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam With this question: CVA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam With this question: CVA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam With this question: CVA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam With this question: CVA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam With this question: CVA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam With this question: CVA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam With this question: CVA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam With this question: CVA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam With this question: CVA 1 (v5.1 + v6.0) Chapter 1 Exam Answers Exam With this question: CVA 1 (v5.1 + v6.0) Chapter 1 (v5.1 Module 5: Network Protocols Quiz Answers Exam with this question: IT Essentials 8.0 Module 9 Quiz Answers: Virtualization and Cloud Computing Exam with this question: IT Essentials 8.0 Module 9 Quiz Answers: Virtualization and Cloud Computing Exam with this question: IT Essentials 8.0 Module 9 Quiz Answers: Virtualization and Cloud Computing Exam with this question: IT Essentials 8.0 Module 9 Quiz Answers: Virtualization and Cloud Computing Exam with this question: IT Essentials 8.0 Module 9 Quiz Answers: Virtualization and Cloud Computing Exam with this question: IT Essentials 8.0 Module 9 Quiz Answers: Virtualization and Cloud Computing Exam with this question: IT Essentials 8.0 Module 9 Quiz Answers: Virtualization and Cloud Computing Exam with this question: IT Essentials 8.0 Module 9 Quiz Answers: Virtualization and Cloud Computing Exam with this question: IT Essentials 8.0 Module 9 Quiz Answers: Virtualization and Cloud Computing Exam with this question: IT Essentials 8.0 Module 9 Quiz Answers: Virtualization and Cloud Computing Exam with this question: IT Essentials 8.0 Module 9 Quiz Answers: Virtualization and Cloud Computing Exam with this question: IT Essentials 8.0 Module 9 Quiz Answers: Virtualization and Cloud Computing Exam with this question: IT Essentials 8.0 Module 9 Quiz Answers: Virtualization and Cloud Computing Exam with the provided ex Quiz Hello friends if you are looking for Cloud TQ Multiple choice questions | Cloud TQ Objective type questions | Cloud TQ Accenture MCQ with answers Ans: define a strategy and roadmap Ans: Artificial intelligence Ans: locations | Cloud TQ Accenture MCQ with answers Ans: define a strategy and roadmap Ans: Artificial intelligence Ans: locations | Cloud TQ Accenture MCQ with answers | Cloud TQ Accenture MCQ wi based on the users location Ans: myNav Ans: infrastructure as a service Ans. It documents expectations of availability , up time and security Ans. Helps asses architect and simulate cloud solution to determine the rightcloud architecture based on our clients business needs Ans . Platform as a service (paas) Ans: elasticity Ans : the degree to which a system can adopt to workload changes byprovisioning and deprovisioning resources automatically Ans . Amazon Web services AWS Ans. Multitenancy Ans: private cloud Ans 75% Ans: internet of things (IOT) Ans. It helps access architect and simulate cloud migration solutions Ans: 95% Ans . It allows multiple customers to share application while retaining dataprivacy Ans . It allows multiple customers to share are server26. An international fast-food chain is struggling to identify clear worldwidetrends in customer preferences due to various countries' data being in differentlanguages. How could a Cloud solution help the company address this problem? Ans: by creating cuisines that are specific to each geographical location Ans. The ability to pay as you go and create another ornaments with littleupfront costs.Ans . COMPANY has implemented our cloud solution at scale and delivered clear business valuesAns: serverless computingAns. Infrastructure as a service (iaaS)Ans. It documents expectations of avaliability, uptime, and security.Ans: it allows multiple customers to share application while retaining dataprivacy Ans. The degree to which a system can adapt to workload changes byprovisioning and deprovisioning resource automaticallyAns . Individual users and devicesAns: by providing a data centric approach that offers more speed agility and security Ans. By bringing multiple services together to serve the client's business needs Ans. It has accelerated the urgency for a business to move to the cloud quickly Ans. Infrastructure as a service (IAAs) Topics relating to Cloud computing Cloud computing enables users to access scalable and on-demand computing resources via the internet, utilizing hardware and software virtualization. It is a rapidly evolving technology capable of delivering extensible services efficiently, supporting a wide range of applications from personal storage solutions to enterprise-level systems. Despite its advantages, cloud computing also faces several challenges. Privacy concerns remain a primary issue, as users often lose direct control over their data once it is stored on servers owned and managed by cloud providers. This loss of control can create uncertainties regarding data privacy, unauthorized access, and compliance with regional regulations such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability models define the boundaries of control and accountability between the cloud provider and the customer, but misunderstandings or mismanagement in these areas can still result in security breaches or accidental data loss. Cloud providers offer tools, such as AWS Artifact (compliance assessments and risk analysis), and Google Assured Workloads (region-specific data compliance), to assist customers in managing compliance requirements. [1][2][3] Security issues in cloud computing are generally categorized into two broad groups. The first involves risks faced by cloud customers, such as misconfigurations, inadequate access controls, and accidental data exposure. These risks are often amplified by human error or a lack of understanding of the shared responsibility model. Security responsibilities also vary depending on the service (IaaS), or Software as a Service (SaaS). In general, cloud providers are responsible for hardware security, physical infrastructure, and software updates, while customers are responsible for data encryption, identity and access management (IAM), and application-level security. [1][2][3] Another significant concern is uncertainty regarding guaranteed Quality of Service (QoS), particularly in multi-tenant environments where resources are shared among customers. Major cloud providers address these concerns through Service Level Agreements (SLAs), which define performance and often offer compensation in the form of service Level Agreements (SLAs), which define performance and often offer compensation in the form of service Level Agreements (SLAs), which define performance and often offer compensation in the form of service Level Agreements (SLAs), which define performance and often offer compensation in the form of service Level Agreements (SLAs), which define performance and uptime guarantees are unmet. remediation processes, supported
by tools such as AWS CloudWatch, Azure Monitor, and Google Cloud Operations Suite, help detect and respond to large-scale failures. Despite these tools, managing QoS in highly distributed and multi-tenant systems remains complex. For latency-sensitive workloads, cloud providers have introduced edge computing solutions, such as AWS Wavelength, Azure Edge Zones, and Google Distributed Cloud Edge, to minimize latency by processing data residency and sovereignty introduce further complexity. Data stored in one region may fall under the legal jurisdiction of that region, creating potential conflicts for organizations operating across multiple geographies. Major cloud providers, such as AWS, Microsoft Azure, and Google Cloud, address these concerns by offering region-specific data centers and compliance management tools designed to align with regional regulations and legal frameworks. [1][2][3] The decision to adopt cloud computing or maintain on-premises infrastructure depends on factors such as scalability, cost structure, latency requirements, regulatory constraints, and infrastructure customization. [4][5][6][7] Organizations with variable or unpredictable workloads, limited capital for upfront investments, or a focus on rapid scalability benefit from cloud adoption. Startups, SaaS companies, and e-commerce platforms often prefer the pay-as-you-go operational expenditure (OpEx) model of cloud infrastructure. Additionally, companies prioritizing global accessibility, remote workforce enablement, disaster recovery, and leveraging advanced services such as AI/ML and analytics are suited for the cloud. In recent years, some cloud providers have started offering specialized services for high-performance computing and low-latency applications, addressing some use cases previously exclusive to on-premises setups. [4][5][6][7] On the other hand, organizations with strict regulatory reguirements, highly predictable workloads or reliance on deeply integrated legacy systems may find cloud infrastructure less suitable. Businesses in industries like defense, government, or those handling highly sensitive data often favor on-premises setups for greater control and data sovereignty. Additionally, companies with ultra-low latency requirements, such as high-frequency trading (HFT) firms, rely on custom hardware (e.g., FPGAs) and physical proximity to exchanges, which most cloud providers cannot fully replicate despite recent advancements. Similarly, tech giants like Google, Meta, and Amazon build their own data centers due to economies of scale, predictable workloads, and the ability to customize hardware and network infrastructure for optimal efficiency. However, these companies also use cloud services selectively for certain workloads and applications are increasingly adopting hybrid cloud architectures, combining on-premises infrastructure with cloud services. This approach allows businesses to balance scalability, cost-effectiveness, and control, offering the benefits of both deployment models while mitigating their respective limitations. [4][5][6][7] According to the 2024 State of the Cloud Report by Flexera, approximately 50% of respondents identified the following top challenges when migrating workloads to public clouds: [8] "Understanding application dependencies" "Comparing on-premise and cloud costs" "Assessing technical feasibility." Cloud computing abstractions aim to simplify resource management, but leaky abstractions can expose underlying complexities. These variations in abstraction dependencies" "Comparing on-premise and cloud costs" "Assessing technical feasibility." architecture. Mitigating leaky abstractions requires users to understand the implementation details and limitations of the cloud services they utilize. [9][10][11] The increased use of cloud computing services to the utmost importance. [12][13] The provider of such services lie in a position such that with the greater use of cloud computing services has given access to a plethora of data.[13] This access has the immense risk of data being disclosed either accidentally or deliberately.[13] The privacy of the companies can be compromised as all the information is sent to the cloud service provider [14] Privacy advocates have criticized the cloud model for giving hosting companies' greater ease to control—and thus, to monitor at will—communication between host company and end user, and access user data (with or without permission). Instances such as the secret NSA program, working with AT&T, and Verizon, which recorded over 10 million telephone calls between American citizens, causes uncertainty among privacy advocates, and the greater powers it gives to telecommunication companies to monitor user activity.[15][16] A cloud service provider (CSP) can complicate data privacy because of the extent of virtualization (virtual machines) and cloud storage used to implement cloud service.[17] CSP operations, customer or tenant data may not remain on the same data center or even within the same provider's cloud; this can lead to legal environment, providers such as Amazon still cater to major markets (typically to the United States and the European Union) by deploying local infrastructure and allowing customers to select "regions and availability zones".[18] Cloud computing poses privacy concerns because the service provider can access the data that is on the cloud at any time. It could accidentally or deliberately alter or even delete information.[19] This becomes a major concern as these service providers employ administrators, which can leave room for potential unwanted disclosure of information on the cloud.[13] Sometimes there can be some technical issues like servers might be down so at that time it becomes difficult to gain access to the resources at any time and from anywhere e.g. non-availability of services can be due to denial of service attack. To use the technique of cloud computing is that it consumes the great power of physical devices such as a smartphone.[14] Many cloud providers can share information with third parties if necessary for purposes of law and order even without a warrant. That is permitted in their privacy policies which users have to agree to before they start using cloud services.[20] There are life-threatening situations in which there is no time to agree to before they start using cloud services.[20] There are life-threatening situations in which there is no time to agree to before they start using cloud services.[20] There are life-threatening situations in which there is no time to agree to before they start using cloud services.[20] There are life-threatening situations in which there is no time to agree to before they start using cloud services.[20] There are life-threatening situations in which there is no time to agree to before they start using cloud services.[20] There are life-threatening situations in which there is no time to agree to before they start using cloud services.[20] There are life-threatening situations in which there is no time to agree to before they start using cloud services.[20] There are life-threatening situations in which there is no time to agree to before they start using cloud services.[20] There are life-threatening situations in which there is no time to agree to before they start using cloud services.[20] There are life-threatening situations in which there is no time to agree to agree to before they start using cloud services.[20] There are life-threatening situations in which there is no time to agree to agr wait for the police to issue a warrant. Many cloud providers can share information immediately with the police in such situations. The Dropbox privacy policy states that [21] We may disclose your information as discussed below ... Law & Order. We may disclose your information to third parties if we determine that such disclosure is reasonably necessary to (a) comply with the law; (b) protect any person from death or serious bodily injury; (c) prevent fraud or abuse of Dropbox's property rights. The Sydney Morning Herald reported about the Mosman bomb hoax, which was a life-threatening situation, that: [22] As to whether NSW Police needed a warrant to access the information it was likely to have, Byrne said it depended on the process taken. "Gmail does set out in their process in terms of their legal disclosure guidelines [that] it can be done by a search warrant ... but there are exceptions that can apply in different parts of the world and different service providers. For example, Facebook generally provides an exception for emergency life threatening situations that are signed off by law enforcement." Another computer forensic expert at iT4ensics, which works for large corporations dealing with matters like internal fraud, Scott Lasak, said that police "would just contact Google" and "being of a police or FBI background Google would assist them" "Whether or not they need to go through warrants or that sort of thing I'm not sure. But even for just an IP address they might not even need a warrant for something like that being of a police background. ... NSW Police would not comment on whether it had received help from Google. The search giant also declined to comment, instead offering a standard statement on how it cooperated with law enforcement. A spokesman for the online users' lobby group Electronic Frontiers Australia, Stephen Collins, said Google was likely to have handed over the need information on the basis of "probable cause or a warrant", which he said was "perfectly legitimate". He also said "It happens with relative frequency. ... Such things are rarely used in Australia for trivial or malevolent purposes." Solutions to privacy in cloud service provider needs to establish clear and relevant policies that describe how the data of each cloud user will be accessed and used.[13] Cloud service users can encrypt data that is processed or stored within the cloud to prevent
unauthorized access.[12][13] Cryptographic encryption mechanisms are certainly the best options. In addition, authentication and integrity protection mechanisms are certainly the best options. modified in transit. Strong authentication is a mandatory requirement for any cloud deployment. User authentication and access control, and specially in the cloud and all of its data are publicly accessible.[23] Biometric identification technologies linking users' biometrics information to their data are available. These technologies use searchable encryption techniques, and perform identification in an encrypted domain so that cloud providers or potential attackers do not gain access to sensitive data or even the contents of the individual queries. To comply with regulations including FISMA, HIPAA, and SOX in the United States, the General Data Protection Regulation in the EU and the credit card industry's PCI DSS, users may have to adopt community or hybrid deployment modes that are typically more expensive and may offer restricted benefits. This is how Google is able to "manage and meet additional government and Rackspace are able to claim PCI compliance. [26] Many providers also obtain a SAS 70 Type II audit, but this has been criticised on the grounds that the hand-picked set of goals and standards determined by the auditor and the audite are often not disclosed and can vary widely set of goals and standards determined by the audit of goals and standards determined by the audit of goals and standards determined by the audite are often not disclosed and can vary widely set of goals and standards determined by the audit of goals and standard [27] Providers typically make this information available on request, under non-disclosure agreement. [28][29] Customers in the EU regulations on export of personal data. [30] A multitude of laws and regulations have forced specific compliance requirements onto many companies that collect, generate or store data. These policies may dictate a wide array of data storage policies, such as how long information must be retained, the process used for deleting data, and even certain recovery plans. Below are some examples of compliance laws or regulations. United States, the Health Insurance Portability and Accountability Act (HIPAA) requires a contingency plan that includes, data backups, data recovery, and data access during emergencies. The privacy laws of Switzerland demand that private data, including emails, be physically stored in Switzerland. In the United Kingdom, the Civil Contingencies Act of 2004 sets forth guidance for a business contingency plan that includes policies for data storage. In a virtualized cloud computing environment, customers may never know exactly where their data is stored. In fact, data may be stored across multiple data centers in an effort to improve reliability, increase performance, and provide redundancies. This geographic dispersion may make it more difficult to ascertain legal jurisdiction if disputes arise.[31] Main article: FedRAMP U.S. Federal Agencies have been directed by the Office of Management Program) to assess and authorize cloud products and services. Federal CIO Steven VanRoekel issued a memorandum to federal agency Chief Information Officers on December 8, 2011 defining how federal agencies should use FedRAMP. FedRAMP. FedRAMP. FedRAMP. FedRAMP. FedRAMP. FedRAMP. FedRAMP. the FIPS 199 moderate categorization. The FedRAMP program has also established a Joint Accreditation standards for 3rd party organizations who perform the assessments of cloud solutions. The JAB also reviews authorization packages, and may grant provisional authorization (to operate). The federal agency consuming the service still has final responsibility for final authorization (to operate.[32] As with other changes in the landscape of computing, certain legal issues arise with cloud computing, including trademark infringement, security concerns and sharing of proprietary data resources. The Electronic Frontier Foundation has criticized the United States government during is the problem of who is in "possession" of the data. If a cloud company is the possessor of the data, the possessor has certain legal rights. If the cloud company is the problem in the legalities of cloud computing is the problem of legal ownership of the data. Many Terms of Service agreements are silent on the question of ownership.[34] These legal issues are not confined to the time period in which the cloud-based application is actively being used. There must also be consideration for what happens when the provider-customer relationship ends. In most cases, this event will be addressed before an application is deployed to the cloud. However, in the case of provider insolvencies or bankruptcy the state of the data may become blurred.[31] Because cloud computing is still relatively new, standards are still being developed.[35] Many cloud platforms and services are proprietary, meaning that they are built on the specific standards, tools and protocols developed by a particular vendor for its particular cloud offering.[35] This can make migrating off a proprietary cloud platform prohibitively complicated and expensive.[35] Three types of vendor lock-in: cloud services tend to be built on one of several possible virtualization platforms, for example VMware or Xen. Migrating from a cloud provider using one platform to a cloud provider using a different platform could be very complicated. Data lock-in: since the cloud is still new, standards of ownership, i.e. who actually owns the data once it lives on a cloud platform, are not yet developed, which could make it complicated if cloud computing users ever decide to move data off of a cloud vendor's platform. Tools lock-in: if tools built to manage a cloud environment are not compatible with different kinds of both virtual and physical infrastructure, those tools will only be able to manage data or apps that live in the vendor's particular cloud environment. Heterogeneous cloud environment that have a type of cloud environment that live in the vendor's particular cloud environment. prevents vendor lock-in, and aligns with enterprise data centers that are operating hybrid cloud models.[37] The absence of vendor lock-in lets cloud administrators select their choice of hypervisors for specific tasks, or to deploy virtualized infrastructures to other enterprises without the need to consider the flavor of hypervisors in the other enterprise.[38] A heterogeneous clouds and software-as-a-service clouds, public clouds and software-as-a-service clouds. Heterogeneous clouds also allow for the use of piece parts, such as hypervisors, servers, and storage, from multiple vendors.[40] Cloud piece parts, such as cloud storage systems, offer APIs but they are often incompatible with each other.[41] The result is complicated migration between backends, and makes it difficult to integrate data spread across various locations.[41] The result is complicated migration between backends, and makes it difficult to integrate data spread across various locations.[41] The result is complicated migration between backends, and makes it difficult to integrate data spread across various locations.[41] The result is complicated migration between backends, and makes it difficult to integrate data spread across various locations.[41] The result is complicated migration between backends, and makes it difficult to integrate data spread across various locations.[41] The result is complicated migration between backends, and makes it difficult to integrate data spread across various locations.[41] The result is complicated migration between backends, and makes it difficult to integrate data spread across various locations.[41] The result is complicated migration between backends, and makes it difficult to integrate data spread across various locations.[41] The result is complicated migration between backends, and makes it difficult to integrate data spread across various locations.[41] The result is complete the spread across various locations.[41] The result is complete the spread across various locations.[41] The result is complete the spread across various locations.[41] The result is complete the spread across various locations.[41] The result is complete the spread across various locations.[41] The result is complete the spread across various locations.[41] The result is complete the spread across various locations.[41] The result is complete the spread across various locations.[41] The result is complete the spread across various locations.[41] The result is complete the spread across various locations.[41] The result is complete the spread across various locations.[41] The solution to this is for clouds to adopt common standards.[41] Heterogeneous cloud computing differs from homogeneous clouds, which have been described as those using consistent building blocks supplied by a single vendor.[42] Intel General Manager of high-density computing, Jason Waxman, is quoted as saying that a homogeneous system of 15,000 servers would cost \$6 million more in capital expenditure and use 1 megawatt of power.[42] Service lock-in within the same vendor occurs when a customer becomes dependent on specific services within a cloud vendor, making it challenging to switch to alternative services within the same vendor occurs when a customer becomes dependent on specific services within a cloud vendor, making it challenging to switch to alternative services within the same vendor occurs when a customer becomes dependent on specific services within a cloud vendor, making it challenging to switch to alternative services within a cloud vendor. Category: Free software for cloud computing Open-source software has provided the foundation for many cloud computing implementations, prominent examples being the Hadoop framework [45] and VMware's Cloud Foundry. [46] In November 2007, the Free Software Foundation
released the Affero General Public License, a version of GPLv3 intended to close a perceived legal loophole associated with free software designed to run over a network.[47] See also: Category:Cloud standards Most cloud providers expose APIs that are typically well documented (often under a Creative Commons license[48]) but also unique to their implementation and thus not interoperable. Some vendors have adopted others' APIs and there are a number of open standards under development, with a view to delivering interoperability and portability.[49] As of November 2012, the Open Standard with broadest industry support is probably OpenStack, founded in 2010 by NASA and Rackspace, and now governed by the OpenStack Foundation.[50] OpenStack supporters include AMD, Intel, Canonical, SUSE Linux, Red Hat, Cisco, Dell, HP, IBM, Yahoo, Huawei and now VMware.[51] Main article: Cloud computing security is generally a desired state of being free from harm (anything that compromises the state of an entity's well-being). As defined in information security, it is a condition in which an information asset is protected against its confidentiality (quality or state of being free from unauthorized or insecure disclosure contrary to the defined access rights as listed in the access control list and or matrix), integrity values) and availability (a desired state of an information resource being accessible only by authorized parties (as listed in access control list and or matrix) in the desired state and at the right time. Security is an important domain in as far as cloud computing is concerned, there are a number of issues to be addressed if the cloud is to be perfectly secure (a condition i doubt will ever be achieved)(Martin Muduva, 2015). As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through adoption of this new model.[52][53] The effectiveness and efficiency of traditional protection mechanisms are being voiced about the security issues introduced through adoption of this new model.[52][53] The effectiveness and efficiency of traditional protection mechanisms are being voiced about the security issues introduced through adoption of this new model.[52][53] The effectiveness and efficiency of traditional protection mechanisms are being voiced about the security issues introduced through adoption of this new model.[52][53] The effectiveness and efficiency of traditional protection mechanisms are being voiced about the security issues introduced through adoption of this new model.[52][53] The effectiveness and efficiency of traditional protection mechanisms are being voiced about the security issues introduced through adoption of this new model.[52][53] The effectiveness and efficiency of traditional protection mechanisms are being voiced about the security issues introduced through adoption of this new model.[52][53] The effectiveness and efficiency of traditional protection mechanisms are being voiced about the security issues introduced through adoption of this new model.[52][53] The effectiveness and efficiency of traditional protection mechanisms are being voiced about the security issues introduced through adoption of this new model.[52][53] The effectiveness and efficiency of traditional protection mechanisms are being voiced about the security issues introduced through adoption of the security issues introduc innovative deployment model can differ widely from those of traditional architectures.[54] An alternative perspective on the topic of cloud security is that this is but another, although quite broad, case of "applied security.[55] The relative security of cloud computing services is a contentious issue that may be delaying its adoption.[56] Physical control of the Private Cloud equipment off site and under someone else's control. Physical control of the Private Cloud equipment off site and under someone else's control. links are not compromised. Issues barring the adoption of cloud computing are due in large part to the private and public sectors' unease surrounding the external management of security-based services. It is the very nature of cloud computing-based services. It is the very nature of cloud computing are due in large part to the private and public sectors' unease surrounding the external management of security-based services. great incentive to cloud computing service providers to prioritize building and maintaining strong management of security, accountability, malicious insiders, management console security, account control, and multitenancy issues. Solutions to various cloud security issues vary, from cryptography, particularly public key infrastructure (PKI), to use of multiple cloud providers, standardization of APIs, and improving virtual machine support.[54][58][59] Cloud computing offers many benefits, but is vulnerable to threats.[60] As cloud computing uses increase, it is likely that more criminals find new ways to exploit system vulnerabilities. Many underlying challenges and risks in cloud computing stakeholders should invest heavily in risk assessment to ensure that the system encrypts to protect data, establishes trusted foundation to secure the platform and infrastructure, and builds higher assurance into auditing to strengthen compliance. Security concerns in cloud computing. A compromised server could significantly harm the users as well as cloud providers. A variety of information could be stolen. These include credit card and social security numbers, addresses, and personal messages. The U.S. now requires cloud providers to notify customers of breaches. Once notified, customers now have to deal with federal investigations. lawsuits and reputational damage. Customer lawsuits and settlements have resulted in over \$1 billion in losses to cloud providers.[61] A cloud providers.[61] A cloud providers and settlements have resulted in over \$1 billion in losses to cloud providers.[61] A cloud providers.[61] A cloud providers.[61] A cloud provider may shut down without warning. For instance, the Anki robot company suddenly went bankrupt in 2019, making 1.5 million robots unresponsive to voice command.[62] Although cloud computing is often assumed to be a form of green computing, there is currently no way to measure how "green" computers are.[63] The primary environmental problem associated with the cloud is energy use. Phil Radford of Greenpeace said "we are concerned that this new explosion in electricity use could lock us into old, polluting energy sources instead of the clean energy available today."[64] Greenpeace ranks the energy usage of the top ten big brands in cloud computing, and successfully urged several companies to switch to clean energy. On December 15, 2011, Greenpeace and Facebook announced together that Facebook an [65][66] Soon thereafter, Apple agreed to make all of its data centers 'coal free' by the end of 2013 and doubled the amount of solar energy by 2020.[68] Citing the servers' effects on the environmental effects of cloud computing, in areas where climate favors natural cooling and renewable electricity is readily available, the environmental effects will be more moderate. (The same holds true for "traditional" data centers.) Thus countries with favorable conditions, such as Finland, [69] Sweden and Switzerland, [70] are trying to attract cloud computing data centers. Energy efficiency in cloud computing can result from energy-aware scheduling and server consolidation.[71] However, in the case of distributed clouds over data centers with different sources of energy including renewable energy, the use of energy efficiency reduction could result in a significant carbon footprint reduction.[72] As with privately purchased hardware, customers can purchase the services of cloud computing for nefarious purposes. This includes password cracking and launching attacks using the purchased service as a command and control channel that issued software updates and malicious instructions to PCs that were infected by the malware.[74] Main article: Corporate governance of information technology The introduction of cloud computing requires an appropriate IT governance model to ensure a secured computing requires an appropriate IT governance model to ensure a secured computing requires an appropriate IT governance model to ensure a secured computing requires an appropriate IT governance model to ensure a secured computing requires an appropriate IT governance model to ensure a secured computing requires an appropriate IT governance model to ensure a secured computing requires an appropriate IT governance model to ensure a secured computing requires an appropriate IT governance model to ensure a secured computing requires and to comply with all relevant organizational information technology policies.[75][76] As such, organizations need a set of capabilities that are essential when effectively implementing and managing cloud services, including demand management, relationship management, risk and compliance management. [77] A danger lies with the explosion of companies joining the growth in cloud computing by becoming providers. However, many of the infrastructural and logistical concerns regarding the operation of cloud computing businesses are still unknown. This over-saturation may have ramifications for the industry as a whole.[78] The increased use of cloud computing businesses are still unknown. to cheaper low storage devices that stream all content via the cloud becoming more popular.[citation needed] In a Wired article, Jake Gardner explains that while unregulated usage makes it difficult for business to evaluate and incorporate it into their business plans.[78] Outside of the information technology and software industry, the term "cloud" can be found to reference a wide range of services, some of which fall under the category of cloud computing, while others do not. The cloud is often used to reference a
wide range of services, some of which fall under the category of cloud computing, while others do not. over the Internet, but is not necessarily a computing resource. The term "cloud" retains the aura of something noumenal and numinous.[79] Examples of service that are sometimes referred to as "the cloud" include, but are not limited to, crowd sourcing, cloud printing, crowd funding, cloud manufacturing.[80][81] Due to its multi-tenant nature and resource sharing, cloud computing must also deal with the "noisy neighbor" effect. This effect in essence indicates that in a shared infrastructure, the activity of a virtual machine on a neighboring core on the same physical host, due to issues such as e.g. cache contamination. Due to the fact that the neighboring VMs may be activated or deactivated at arbitrary times, the result is an increased variation in the actual performance of cloud resources. This effect seems to be dependent on the nature of the applications that run inside the VMs but also other factors such as scheduling parameters and the careful selection may lead to optimized assignment in order to minimize the phenomenon. This has also led to difficulties in comparing various cloud providers on cost and performance, as the time period and location in which the benchmark is performed can result in widely varied results.[82] This observation has led in turn to research efforts to make cloud computing applications intrinsically aware of changes in the infrastructure so that the application can automatically adapt to avoid failure.[83] Philosopher Slavoj Žižek points out that, although cloud computing applications intrinsically aware of changes in the infrastructure so that the application can automatically adapt to avoid failure. grounded in the virtually monopolistic privatization of the cloud which provides this access. According to him, this access, necessarily mediated through a handful of companies, ensures a progressive privatization of global cyberspace. Žižek criticizes the argument purport of the cloud computing that this phenomenon is part of the "natural evolution" of the Internet, sustaining that the quasi-monopolies "set prices at will but also filter the software they provide to give its "universality" a particular twist depending on commercial and ideological interests."[84] Typically, cloud providers' Service Level Agreements (SLAs) do not encompass all forms of service interruptions Exclusions typically include planned maintenance, downtime resulting from external factors such as network issues, human errors, like misconfigurations, natural disasters, force majeure events, or security breaches. Typically, customers bear the responsibility of monitoring SLA compliance and must file claims for any unmet SLAs within a nated timeframe. Customers should be aware of how deviations from SLAs are calculated, as these parameters may vary by service. These requirements can place a considerable burden on customers. Additionally, SLA percentages and conditions can differ across various services within the same provider, with some services lacking any SLA altogether. In cases of service interruptions due to hardware failures in the cloud provider, the company typically does not offer monetary compensation. Instead, eligible users may receive credits as outlined in the corresponding SLA. [85][86][87][88] In a report by Gartner, a survey of 200 IT leaders revealed that 69% experienced budget overruns in their organizations' cloud expenditures during 2023. Conversely, 31% of IT leaders whose organizations stayed within budget attributed their success to accurate forecasting and budgeting, proactive monitoring of spending, and effective optimization. [89] The 2024 Flexera State of Cloud Report identifies the top cloud challenges as managing cloud spend, followed by security concerns and lack of expertise. Public cloud expenditures exceeded budgeted amounts by an average of 15%. The report also reveals that cost savings, while 42% prioritize shorter time-to-market, indicating that cloud's promise of accelerated deployment is often overshadowed by cost concerns. [8] Applications hosted in the cloud are susceptible to the fallacies of distributed computing, a series of misconceptions that can lead to significant issues in software development and deployment. Mahmood, Zaigham (2013). Cloud Computing: Concepts, Technology & Architecture. Pearson Education. ISBN 978-0133387520. ^ a b c d Ruparelia, Nayan B. (August 2023). Cloud Computing: Theory and Practice. Elsevier Science. ISBN 978-0124046276. ^ a b c d Hurwitz, Judith S.; Bloor, Robin; Kaufman, Marcia; Halper, Fern (16 November 2009). Cloud for Architects: Build robust hybrid cloud solutions using AWS and OpenStack. Packt ISBN 9781788623513. ^ a b c d Buckwell, Mark; Daele, Stefaan van; Horst, Carsten (3 September 2024). Security Architecture for Hybrid Cloud: A Practical Method for Designing Security Using Zero Trust Principles. O'Reilly Media. ISBN 9781098157777. ^ a b c d Kavis, Michael J. (28 January 2014). Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS). John Wiley & Sons. ISBN 978-1118617618. ^ a b "2024 State of the Cloud Report". Flexera's State of the Cloud Report". Flexera's State of the Cloud Report". Flexera's State of the Cloud Report. ^ Cloud Native Infrastructure: Patterns for Scalable Infrastructure: Patterns for Scalab Hausenblas, Michael (26 December 2023). Cloud Observability in Action. Simon and Schuster. ISBN 9781633439597. ^ Jr, Cloves Carneiro; Schmelmer, Tim (10 December 2016). Microservices From Day One: Build robust and scalable software from the start. Apress. ISBN 9781484219379. ^ a b Haghighat, Mohammad; Zonouz, Saman; Abdel-Mottaleb, Mohamed (2015). "CloudID: Trustworthy cloud-based and cross-enterprise biometric identification". Expert Systems with Applications. 42 (21): 7905-7916. doi:10.1016/j.eswa.2015.06.025. ^ a b c d e f g ryan, mark (January 2011). "Cloud Computing Privacy Concerns on Our Doorstep". ACM. 54: 36-38. doi:10.1145/1866739.1866751. ^ a b Anushka Gaur, Anurag Jain. Glimpse of Cloud Computing, International Journal of Advance Research, Ideas and Innovations in Technology, www.IJARIIT.com. ^ Cauley, Leslie (2006-05-11). "NSA has massive database of Americans' phone calls". USA Today. Retrieved 2010-08-22. ^ "NSA taps in to user data of Facebook, Google and others, secret files reveal". 2013-06-07. Retrieved 2013-06-07. ^ Winkler, Vic (2011). Securing the Cloud: Cloud Computer Security Techniques and Tactics. Waltham, Massachusetts: Elsevier. p. 60. ISBN 978-1-59749-592-9. Archived from the original on 2012-07-29. Retrieved 2014-07-03. ^ "Regions and Availability Zones". Amazon Web Services Documentation Retrieved 2014-01-24. ^ "Cloud Computing Privacy Concerns on Our Doorstep". January 2011. ^ All Cloud Drives from One Location. Retrieved 2014-12-04. ^ "Every touch leaves a trace': how Google helped track bomb hoax suspect". 2011-08-17. Retrieved 2014-12-04. ^ Sen, Saydip (2013). "Security and Privacy Issues in Cloud Computing". In Ruiz-Martinez; Pereniguez-Garcia; Marin-Lopez (eds.). Architectures and Protocols for Secure Information Technology Infrastructures. Advances in Information Security, Privacy, and Ethics. USA: IGI-Global. pp. 1–45. arXiv:1303.4814. Bibcode:2013arXiv1303.4814S. doi:10.4018/978-1-4666-4514-1.ch001. ISBN 9781466645141. S2CID 14091704. ^ "FISMA compliance for federal cloud computing on the horizon in 2010-08-22. ^ "Cloud Hosting is Secure for Take-off: Mosso Enables The Spreadsheet Store, an Online Merchant, to become PCI Compliant". Rackspace. 2009-03-14. Archived from the original on 2011-10-01. Retrieved 2010-08-22. ^ "Assessing Cloud Computing Agreements and Controls". WTN News, Archived from the original on 2011-04-03. Retrieved 2010-08-22. ^ "Cloud Certification From Competitive Differentiator". Cloudcor, 20 September 2011. Retrieved 2011-09-20. ^ "How the New EU Rules on Data Export Affect Companies in and Outside the EU | Dr. Thomas Helbing - Kanzlei für Datenschutz-, Online- und IT-Recht". Dr. Thomas Helbing. Retrieved 2010-08-22. ^ a b Chambers, Don (July 2010). "Windows Azure: Using Windows Azure: Archived from the original on 2012-10-06. Retrieved 2012-06-17. ^ Cohn, Cindy; Samuels, Julie (31 October 2012). "Megaupload and the Government's Attack on Cloud Computing". Electronic Frontier Foundation. Retrieved 2012-12-14. ^ Maltais, Michelle (26 April 2012). "Who owns your stuff in the cloud?". Los Angeles Times. Retrieved 2012-12-14. 14. ^ a b c McKendrick, Joe. (2011-11-20) "Cloud Computing's Vendor Lock-In Problem: Why the Industry is Taking a Step Backward," Forbes.com [1] ^ Hinkle, Mark. (2010-6-9) "Three cloud lock-in considerations", Zenoss Blog [2] ^ Staten, James (2012-07-23). "Gelsinger brings the 'H' word to VMware". ZDNet. [3] ^ Vada, Eirik T. (2012-06-11) "Creating Flexible Heterogeneous Cloud Environments", page 5, Network and System Administration, Oslo University College [4] ^ Geada, Dave. (June 2, 2011) "The case for the heterogeneous cloud," Cloud Computing in 2012: What's Already Happening". Neovise.[6] Archived 2014-07-01 at the Wayback Machine ^ a b c d Livenson, Ilja. Laure, Erwin. (2011) "Towards transparent integration of heterogeneous cloud, storage platforms", pages 27-34, KTH Royal Institute of Technology, Stockholm, Sweden. [7] ^ a b Gannes, Liz. GigaOm, "Structure 2010: Intel vs. the Homogeneous Cloud," June 24, 2010. [8] ^ Jennings, Roger (29 December 2010). Cloud Computing with the Windows Azure Platform. John Wiley & Sons. ISBN 9781118058756. ^ Schulz, Greg (25 August 2011). Cloud and Virtual Data Storage Networking. CRC Press. ISBN 9781466508446. ^ Jon Brodkin (July 28, 2008). "Open source fuels growth of cloud computing, software-as-a-service". Network World. Archived from the original on October 15, 2012. Retrieved 2012-12-14. ^ "AGPL: Open Source Licensing in a Networked Age". Redmonk.com.
2009-04-15. Retrieved 2010-08-22. ^ GoGrid Moves API Specification to Creative Commons Archived May 5, 2009, at the Wayback Machine ^ "Eucalyptus Completes Amazon Web Services Specs with Latest Release". Ostatic.com. Archived from the original on 2012-10-08. Retrieved 2010-08-22. ^ "OpenStack Foundation launches". Infoworld.com. 2012-09-19. Retrieved 2012-11-17. ^ "Did OpenStack Let VMware Into The Henhouse?". InformationWeek. 2012-10-19. Retrieved 2012-11-17. ^ a b Mariana Carroll; Paula Kotzé; Alta van der Merwe (2012). "Securing Virtual and Cloud Environments". In I. Ivanov; et al. (eds.). Cloud Computing and Service Science, Service S doi:10.1007/978-1-4614-2326-3. ISBN 978-1-4614-2325-6. S2CID 45153604. ^ M Carroll, P Kotzé, Alta van der Merwe (2011), Secure virtualization: benefits, risks and constraints, 1st International Conference on Cloud Computing and Services Science, Noordwijkerhout, The Netherlands, 7–9 May 2011 ^ a b Zissis, Dimitrios; Lekkas (2010). "Addressing cloud computing security issues". Future Generation Computer Systems. 28 (3): 583. doi:10.1016/j.future.2010.12.006. Winkler, Vic (2011). Security Techniques and Tactics. Waltham, MA USA: Syngress. pp. 187, 189. ISBN 978-1-59749-592-9. Archived from the original on 2012-07-29. Retrieved 2014-07-03. ^ "Are security issues delaying adoption of cloud computing?". Network World. Archived from the original on 2010-02-22. Retrieved 2010-08-22. ^ "Security of virtualization, cloud computing divides IT and security pros". Network World. 2010-02-22. Retrieved 2010-08-22. ^ "Security of virtualization, cloud computing divides IT and security pros". Network World. 2010-02-22. Retrieved 2010-08-22. ^ "Security of virtualization, cloud computing divides IT and security pros". Network World. 2010-02-22. Retrieved 2010-08-22. ^ "Security of virtualization, cloud computing divides IT and security pros". Network World. 2010-02-22. Retrieved 2010-08-22. ^ "Security of virtualization, cloud computing divides IT and security pros". Network World. 2010-02-22. Retrieved 2010-08-22. ^ "Security of virtualization, cloud computing divides IT and security pros". Network World. 2010-02-22. Retrieved 2010-08-22. ^ "Security of virtualization, cloud computing divides IT and security pros". Network World. 2010-02-22. Retrieved 2010-08-22. ^ "Security of virtualization, cloud computing divides IT and security pros". Network World. 2010-02-22. Retrieved 2010-08-22. ^ "Security of virtualization, cloud computing divides IT and security pros". Network World. 2010-02-22. Retrieved 2010-08-22. ^ "Security of virtualization, cloud computing divides IT and security pros". Network World. 2010-02-22. Retrieved 2010-08-22. ^ "Security of virtualization, cloud computing divides IT and security pros". Network World. 2010-02-22. Retrieved 2010-08-22. ^ "Security of virtualization, cloud computing divides IT and security pros". Network World. 2010-02-22. Retrieved 2010-08-22. ^ "Security of virtualization, cloud computing divides IT and security pros". Network World. 2010-02-22. Retrieved 2010-08-22. ^ "Security of virtualization, cloud computing divides IT and security pros". Network World. 2010-02-22. Retrieved 2010-08-22. ^ "Security of virtualization, cloud computing divides IT and security pros". Network World. 2010-08-22. ^ "Securi Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Zaharia, M. (2010). "A view of cloud computing". Communications of the ACM. 53 (4): 50-58. doi:10.1145/1721654.1721672. Anthens, G (2010). "Security in the cloud". Communications of the ACM. 53 (11): 16. doi:10.1145/1839676.1839683. S2CID 9125453. Solomon, Amiad. "Importance of Cloud Cost Management". Spot by NetApp. Retrieved 2022-08-12. > Bowen, Janine Anthony. (2011). Cloud Computing: Issues in Data Privacy/Security and Commercial Considerations. Computer and Internet Lawyer Trade Journal. 28 (8), 8. > "Inside Anki shutdown: Who owns IP, assets auction, failed partnership". 2019-06-18. > Iames Urguhart (Ianuary 7, 2019-06-18. > Iames Urguh 2010). "Cloud computing's green paradox". CNET News. Retrieved March 12, 2010. ... there is some significant evidence that the cloud is encouraging more compute consumption ^ "Dirty Data Report Card" (PDF). Greenpeace. Retrieved 2013-08-22. ^ "Facebook and Greenpeace settle Clean Energy Feud". Techcrunch. 15 December 2011. Retrieved 2013-08-22. ^ "Facebook Commits to Clean Energy Future". Greenpeace. Retrieved 2013-08-22. ^ "Salesforce Announces Commitment to a Cloud Powered by 100% Renewable Energy". Greenpeace. 2013-03-06. Archived from the original on 2018-10-22. Retrieved 2013-08-22. ^ Finland - First Choice for Siting Your Cloud Computing Data Center. Archived 2013-07-06 at the Wayback Machine. Retrieved 4 August 2010. ^ Swiss Carbon-Neutral Servers Hit the Cloud... Retrieved 4 August 2010. ^ Berl, Andreas, et al., Energy-Efficient Cloud Computing, The Computer Journal, 2010. ^ Farrahi Moghaddam, Fereydoun, et al., Low Carbon Virtual Private Clouds, IEEE Cloud 2011. ^ Alpeyev, Pavel (2011-05-14). "PlayStation Network hack launched from Amazon EC2". The Register. Retrieved 2011-05-14). "PlayStation Network hack launched from Amazon EC2". The Register. Retrieved 2011-05-14). "Amazon.com Server Said to Have Been Used in Sony Attack". 2012-05-18. ^ Hsu, Wen-Hsi L., "Conceptual Framework of Cloud Computing Governance Model - An Education Perspective", IEEE Technology and Engineering Education (ITEE), Vol 7, No 2 (2012) "Conceptual Framework of Cloud Computing Governance Model - An Education Perspective", IEEE Technology and Engineering Education (ITEE), Vol 7, No 2 (2012) "Conceptual Framework of Cloud Computing Governance Model - An Education Perspective", IEEE Technology and Engineering Education (ITEE), Vol 7, No 2 (2012) "Conceptual Framework of Cloud Computing Governance Model - An Education Perspective", IEEE Technology and Engineering Education (ITEE), Vol 7, No 2 (2012) "Conceptual Framework of Cloud Computing Governance Model - An Education Perspective", IEEE Technology and Engineering Education (ITEE), Vol 7, No 2 (2012) "Conceptual Framework of Cloud Computing Governance Model - An Education Perspective", IEEE Technology and Engineering Education (ITEE), Vol 7, No 2 (2012) "Conceptual Framework of Cloud Computing Governance Model - An Education Perspective", IEEE Technology and Engineering Education (ITEE), Vol 7, No 2 (2012) "Conceptual Framework of Cloud Computing Governance Model - An Education Perspective", IEEE Technology and Engineering Education (ITEE), Vol 7, No 2 (2012) "Conceptual Framework of Cloud Computing Governance Model - An Education Perspective", IEEE Technology and Engineering Education (ITEE), Vol 7, No 2 (2012) "Conceptual Framework of Cloud Computing Governance Model - An Education Perspective", IEEE Technology and Engineering Education (ITEE), Vol 7, No 2 (2012) "Conceptual Framework of Cloud Computing Governance Model - An Education Perspective", IEEE Technology and Engineering Education (ITEE), Vol 7, No 2 (2012) "Conceptual Framework of Cloud Computing Governance Model - An Education Perspective", IEEE Technology and Engineering Education (ITEE), Vol 7, No 2 (2012) "Conceptual Framework of Cloud Computing Governance Model - An Education (ITEE), Vol 7, No 2 (2012) "Conceptual Framework of Cloud Computing Go 07-03. ^ Stackpole, Beth, "Governance Meets Cloud: Top Misconceptions", InformationWeek, 7 May 2012 [9] ^ Joha, A and M. Janssen (2012) "Transformation to Cloud Services Sourcing: Required IT Governance Capabilities", ICST Transactions on e-Business 12(7-9) [10] ^ a b Gardner, Jake (2013-03-28). "Beware: 7 Sins of Cloud Computing". Wired. Retrieved 2013-06-20. ^ Bicudo de Castro, Vicente; Coelho, Heitor; Bantim Frambach, Danilo (2023-07-08). "Wistification: The Dreadful Side of Cloud Computing". Coolabah (34): 91-111. doi:10.1344/co20233491-111. ISSN 1988-5946. ^ S. Stonham and S. Nahalkova (2012) "What is the Cloud and how can it help my business?" "What is the Cloud? How can the Cloud help my business? | OVASTO - Business and Marketing Strategy". Archived from the original on 2014-07-03. ^ S. Stonham and S. Nahalkova (2012), Whitepaper "Tomorrow Belongs to the Agile (PDF)" "Developing Cloud Strategies for Business Agility | OVASTO". Archived from the original on 2013-11-06. Retrieved 2014-07-03. ^ George Kousiouris, Tommaso Cucinotta, Theodora Varvarigou, "The Effects of Scheduling, Workload Type and Consolidation Scenarios on Virtual Machine Performance and their Prediction through Optimized Artificial Neural Networks"[11], The Journal of Systems and Software (2011), Volume 84, Issue 8, August 2011, pp. 1270-1291, Elsevier, doi:10.1016/j.jss.2011.04.013. ^ "Archived copy". Archived from the original on 2020-08-14. Retrieved 2022-06-29. {{cite web}}: CS1 maint: archived copy as title (link) ^ Slavoj Žižek (May 2, 2011). "Corporate Rule of Cyberspace". Inside Higher Ed. Retrieved July 10, 2013. ^ Cloud Security and Privacy An Enterprise Perspective on Risks and Compliance. O'Reilly Media. 4 September 2009. ISBN 9781449379513. ^ Requirements Engineering for Service and Cloud Computing Basics. Springer. ISBN 9781461476993. ^ Murugesan, San (August 2016). Encyclopedia of Cloud Computing. John Wiley & Sons. ISBN 9781118821978. ^ "2024 Cloud Spending: IT Balances Costs with GenAI Innovation". Gartner Peer Community. Retrieved from " Have you ever thought about how cloud computing started? Who came up with the idea? How did it grow into the services we use every day, like Netflix, Google Drive, and AWS? Today, it's very easy to use computers, storage, and apps from anywhere in the world without buying expensive equipment or setting up complicated systems. But a few years ago, this idea was completely new and surprising to everyone. Imagine it's the 1990s, and you want to store 1000 photos. You would need to buy a big hard drive and set it up at home. Today, with cloud services like Google Drive, you can just upload your
photos online and access them anytime, anywhere, no need to buy a big hard drive and set it up at home. cloud computing, and that's what we are going to explore. In this article, we will cover the basic overview of cloud computing, and will cover the history of cloud computing, and vill cover the basic overview of cloud computing. Let's discuss it one by one. Cloud ComputingCloud Computing referred as the accessing and storing of data and provide services related to computing over the internet. It is simply referred to as remote services on the internet. It is simply referred to as remote services on the internet. Cloud computing is in huge demand so, big organization providing the service like Amazon AWS, Microsoft Azure, Google Cloud, Alibaba cloud etc. are some Cloud computing. And also cover the history of client server computing, distributed computing, and cloud computing. Before Computing was come into existence, client Server Architecture was used where all the data and control of client resides in Server and after that user will get appropriate access. But it has many disadvantages. So, After Client Server computing, Distributed Computing was come into existence, in this type of computing all computers are networked together with the help of this, user can share their resources when needed. It also has certain limitations. So in order to remove limitations faced in distributed system, cloud computing was emerged. During 1961, John MacCharty delivered his speech at MIT that "Computing Can be sold as a Utility, like Water and Electricity." According to John MacCharty it was a brilliant idea. But people at that time don't want to adopt this technology. They thought the technology they are using efficient enough for them. So, this concept of computing was not appreciated much so and very less will

research on it. But as the time fleet the technology caught the idea after few years this idea is implemented. So, this is implemented by Salesforce.com in 1999. This company started delivering an enterprise application over the internet and this way the boom of Cloud Computing was started. In 2002, Amazon started Amazon Web Services (AWS), Amazon will provide storage, computation over the internet. In 2006 Amazon will launch Elastic Compute Cloud Commercial Service which is open for Everybody to use. After that in 2009, Google Play also started providing Cloud Computing Enterprise Application as other companies will see the emergence of cloud Computing they also started providing their cloud services. Thus, in 2009, Microsoft launch Microsoft Azure and after that other companies like Alibaba, IBM, Oracle, HP also introduces their Cloud Services. In today the Cloud Computing become very popular and important skill.Advantages The following are some of the benefits of using cloud computing: It seasier to get backup in cloud. It allows us easy and quick access stored information anywhere and anytime. It allows us to access data via mobile. It reduces both hardware ad Software cost, and it is easily maintainable. One of the biggest advantage of Cloud Computing is Database Security. Disadvantages The following are some of disadvantages you will face while using cloud computing: It requires good internet connection. User have limited control on the data. ConclusionCloud computing has evolved from a visionary concept in the 1960s to an integral part of today's digital world. It enables flexible, scalable, and cost-effective access to computing resources, transforming how we store data, run applications, and deliver services.