Paper 1: Security and Privacy Aspects of Cloud Computing: A Smart Campus Case Study

Abstract

The trend of cloud computing is accelerating along with emerging technologies such as utility computing, grid computing, and distributed computing. Cloud computing is showing remarkable potential to provide flexible, cost effective, and powerful resources across the internet, and is a driving force in today's most prominent computing technologies. The cloud offers the means to remotely access and store data while virtual machines access data over a network resource.

Problem

Data security threats can be categorized as external or internal in the cloud environment. Internal threats occur mainly from insider attacks, and external threats from outside attacks as data is accessed by a third party. Attackers can obtain the personal information of a user. The cloud infrastructure should be scalable to ensure availability of data. Six major security issues are listed below :

- Data integrity
- Data privacy and confidentiality
- Location of data
- Availability of data
- Data storage, backup, and recovery ● Data authentication..

Key Idea

However, cloud service providers have not been providing enough secure and reliable services to end users. Blockchain is a technology that is improving cloud computing. This revolutionary technology offers persuasive data integrity properties and is used to tackle security problems. This research presents a detailed analysis of privacy and security challenges in the cloud.

Nature of problem

- Date confidentiality
- Web service security
- Uncertainty in service of realibility
- Unauthorized access
- Data forgery
- Malicious attack
- Ddos
- Loss of data integrity and confidantialty

Suggested solutions

- Hashing and encryption.
- SSL/TSL for client authentication.
- Authorization and authentication.
- Fragmentation redundancy and scattering techniques.
- Enforcement of access policies.
- Fuzzy logic-based mechanism
- IPS and IDS
- Enforcement of access policies.
- Proper integration and confidentiality mechanism.

Critique

We studied its security and privacy through a case study in a smart campus scenario. We seek to highlight the major security vulnerabilities in cloud computing since it has become the most commonly used method of virtualization in large and modern data centers and cloud infrastructures. The major threats and open security issues are a breach of data, IP spoofing, ARP spoofing, DNS poisoning, injection with SQL, injection with OS, LDAP injection, orchestration of the cloud, and zombies or DDoS. Jain and Jaiswal emphasized cloud security parameters: cloud network, database, operating system, virtualization, resource allocation, transaction management, load balancing, memory management, and concurrency control.

Paper 2: Resolving The Security and Data Concerns in Cloud Computing by Utilizing Decentralized Cloud Computing Option

Abstract

There are a variety of security concerns around cloud computing infrastructure technology. Some of these include infrastructure security against threats, data privacy, integrity, and infrastructure stability. In modern cloud computing, there are two models that cloud computing infrastructures follow: centralized cloud computing and decentralized cloud computing. Centralized cloud computing is susceptible to outages, data breaches, and other security threats. Decentralized cloud computing is more resilient to outages due to georedundancy technology, and data is better protected by encryption through Reid Solomon erasure coding.

Problem

Regardless of the type of cloud computing infrastructure, users and enterprises alike are heavily concerned with a variety of security concerns, both regarding cybersecurity attacks, data privacy and integrity, and cloud computing infrastructure stability. Since cloud computing resources can be accessed from around the world, data privacy is often the foremost concern of users and enterprises.

Key Idea

There are a variety of security concerns around cloud computing infrastructure technology. Some of these include infrastructure security against threats, data privacy etc. These problems could be tackled by implementing the decentralized models of cloud computing technologies.

Novelty

There are new types of cybersecurity threats emerging every day as new technology develops and evolves. Cloud computing is not immune to traditional cybersecurity threats, and in fact, is more susceptible to certain types of threats.

Phishing: Phishing refers to the practice of sending fraudulent information or messages that appear to be from genuine, trusted sources in an attempt to elicit sensitive information from the target.

Ransomware: Ransomware refers to malicious computer programs or software that prevent the user from using the computer or workstation until a sum of money or another demand is relinquished.

Trojan: In Cybersecurity, Trojan refers to a malicious computer program or software that is packaged to appear as if it is a useful, legitimate piece of software but in the background runs malicious processes meant to record sensitive information and relay it back to the distributor.

Botnet: A botnet refers to a private network of computers that have all been infected with a harmful or malicious piece of software and controlled in unison for unwanted activity such as mass distribution of spam messages.

Distributed Denial of Service: A distributed denial of service attack refers to a malicious attack meant to disturb a network service or resource by flooding the resource with inbound requests to overload its resources and make it unavailable to legitimate requests.

Crypto-mining: Crypto-mining refers to the practice of using computers for the mining of cryptocurrency without the user's knowledge. This results in a monetary gain for the party who deployed the crypto mining malicious software.

Critique

A decentralized cloud computing infrastructure does not provoke the same stability concerns that the centralized cloud computing model does. Decentralized cloud computing infrastructures use geo-redundant resources, which means that if one resource or region goes down, traffic is routed to another region where data and resources are still accessible and available.[3] This is because decentralized cloud computing replicates resources and data across different locations automatically, eliminating outages unless a significant amount of the locations are experiencing outages. Each location is often located in drastically different places than the other locations, such as in entirely different locations rather than just different buildings. This means there is no single point of failure for a decentralized cloud computing infrastructure, giving decentralized cloud computing high stability in comparison to traditional centralized cloud computing infrastructures.

Paper 3: A Concise Review of Big Data and Cloud Computing Paradigms and Principles

Abstract:

Big data is one of the most important new technologies right now. Big Data is a term that refers to the inadequacy of existing data architectures to manage large data sets efficiently. The 4Vs of big data — volume, velocity, variety, and veracity – make traditional data warehouses difficult to manage and analyze. It's critical to consider big data and analytics in tandem. The term "big data" refers to the recent proliferation of various forms of data from many sources. Big data systems (such as Hadoop) are built on the shared nothing principle, where each node is independent and self-sufficient. Businesses and educational institutions can have a better future path by combining big data and cloud computing technology.

Problem

The Big Data Analysis paradigm has been hampered by serious underlying data privacy issues which are present in practically all ICT innovations, not only Big Data. It involves questions of :

- Confidentiality (who owns the data generated?).
- Who owns the data analysis results?), and
- Integrity (who guarantees the data's accuracy?
- Interoperability (who sets the standards for data exchange?) and
- False positive data analysis (who would be responsible for that?). as well as accessibility. Variety of Big data – Structured, unstructured and semi structured data
- Volume of Big data –Speed of data generation
- Value of Big data – Extracting useful information and making it valuable ● Velocity of Big data – Speed of data generation

Key Idea

Cloud computing also offers virtualization technology that gives users the ability to select any of the following: operating systems, applications, and any of the following: operating systems, applications, and network interconnects additional software flexibility for theirmodest rental fee. Therefore the solution to big data lies in cloud computing.

Novelty

The three main terms that generally signifying new Big Data Challenges are:

i. Volume: This has to do with the amount of data generated on a daily basis which is so large and keeps increasing with time.

ii. Variety: Today data is created in different type, form and formats such as emails, video iii. Velocity: This has to do with the speed it takes to produce data and how fast this data produced needs to be processed on time to meet individual demand.

The other two properties that need to be critically consider when talking about Big Data are Variability and Complexity

Variability: this goes along with velocity, and it has to do with how inconsistent the flow of data can be with respect to time and far it can go.

ii. Complexity: the complexity of the data must be onsidered especially when we have multiple source of data. The data must be rearranged in such a format that will be suitable for processing.

Critique

No need of powerful and expensive computers of large amounts of memory and disks. CD and DVD are not necessary as all the information and programs remain in the cloud. The users can use a compact netbook. Also,It is faster and cheaper to develop applications to test a server under load and to offer customers their solutions directly in the cloud

But, Functionality of cloud services. Not all software applications and their functionalities are available in the cloud. For example, Google Docs app or Office web application have fewer features and capabilities when compared to those of Microsoft Excel.And, To identify the applications that will run in the cloud.

To examine and analyze the existing IT structure of the company in order to determine where changes make sense. For example, Web applications can be transferred to the cloud, while the desktop applications (word processing and graphics) can stay with the end user.

Paper 4: A Study of Role and Impact of Cloud Computing in Supply Chain Management

Abstract

The purpose of this review is to examine the collaborative benefits and social outcomes that associations derive from strong collaborative relationships. Competition between businesses such as multi-connected supply chains has increased the dependence between business connections and has become a key process for partnerships. the cloud could operate with coordinated efforts across the branch network, although there are conflicting prospects for cloud profitability. This concentrate also assesses the impact that distributed IT innovations have on collaborative utility and social outcomes in small and large partnerships.

Problem

Mitigating and accounting for unforeseen delays somewhere along the chain. This is the most common issue that arises within any supply chain, and it's also the one that can be the hardest to predict and safeguard against. There are so many potential issues that can impact a supply chain to cause delays (such as fluctuating availability of raw materials, hold-ups in customs, adverse weather, staffing problems, political issues, procurement problems, changes in legislation and so on) that being able to realistically foresee and safeguard against each of them will only ever be partially successful, and it takes up a lot of resources.

Key Idea

Employing cloud-based technology in supply chains could generate numerous advantages such as capital investment savings, simplified operations, scalability, real-time visibility, as well as sustainability.A cloud supply chain is two or more parties linked by the provision of cloud services, related information and funds.. However, before shifting from a traditional supply chain to a cloud supply chain, companies should first identify the technical requirements for migrating supply chain activities to the cloud.

Novelty

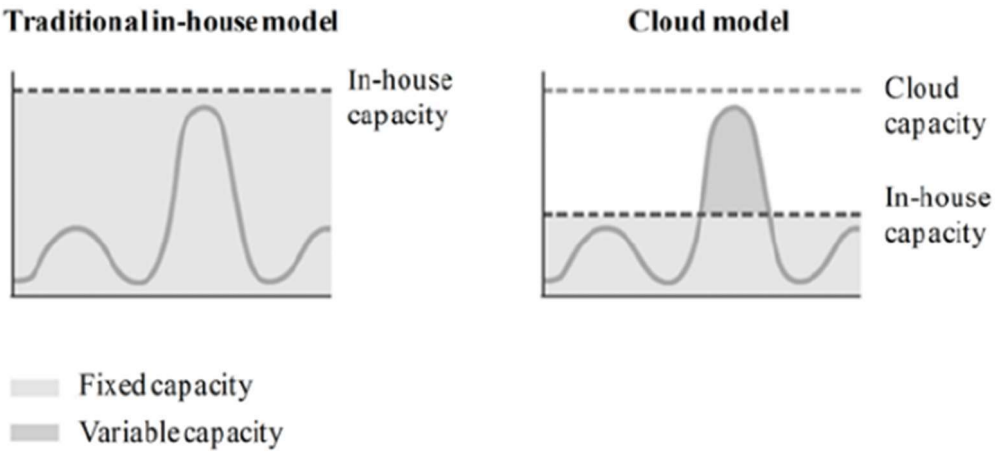
What's new is that, Cloud computing systems can be used effectively in supply chain management as involved companies can highly benefit from the derived financial advantages. With the help of cloud technologies, accessible through the same platform, eliminating compatibility problems as well as providing easy connection and enabling supply chain

information sharing among partners in one single supply chain system. By employing cloud computing, supply chain stakeholders can control their system capacity more accurately, in times of high demands, by using common on-premises systems, they should own the necessary database for the whole year in order to respond to the excessive demand.

Critique

The most common challenges and limitations that companies face when using cloud-based technologies are data security and privacy.cloud computing systems as software products cannot always ensure confidentiality and as a result run increasing risk of being infiltrated by hacking systems. Additionally, possible data acquisition by competing companies would pose an imminent threat to the whole supply chain

Traditional in-house model vs. hybrid cloud model (adapted from M&E Team, 2009)



Also,due to the fact that manufacturing is a complex core procedure that consists of individualized processes depending on each company's products, it requires a high degree of customization that cloud-based services cannot offer yet.

Paper 5: The Evolution Of AI Cloud Computing And The Future It Holds

Abstract

Artificial Intelligence in Cloud Computing is a growing field that focuses on building intelligent solutions for myriad industries. Advanced calculations that companies can use to create dynamic applications. AI Cloud Computing focuses on building those intelligent applications, helping companies use Big Data, deploy algorithms for advanced app functionality, and predict and forecast future growth that tremendously helps with business profitability and longevity. here, we explores the evolution of AI in Cloud Computing, its benefits for small and large enterprises, the latest market trends, use cases, and future predictions.

Problem

Moving AI workloads to the cloud is one of the biggest challenges we see companies facing. Many have data stored across silos, whether it's in the cloud, in HDFS clusters, on-premises. Training models have more data than ever before, but that data is increasingly distributed and the number of queries is growing fast, putting more load on systems. Hybrid latency prevents companies from running AI workloads in the cloud with data on-prem. So, most copy data into the cloud and maintain that duplicate data. And companies with compliance/data sovereignty requirements may even prevent organizations from copying that data. All of this means it is challenging to make both on-prem HDFS AI data accessible and high performing.

Key Idea

AI paired with Cloud Computing offers an enhanced capability for storing and processing data while Machine Learning tools constantly learn and improve operational efficiency. With tools like IBM Watson, Microsoft Azure, and Google Cloud AI, small and large companies have a plethora of enhanced functionalities to upgrade their systems for better productivity.

Novelty

In other sectors, the significant expense a business has to bear is the upfront costs like maintaining on-site data centers. AI-based Cloud projects eliminate those costs. The on-site data centers are not only hard to manage in terms of workloads but may also pose myriad security risks that can lead to significant data loss. With AI Cloud Computing, companies can access AI-powered tools at a monthly cost, which not only enhances overall productivity and security but also enables companies to derive valuable insights through AI-powered data analytics.

AI can perform complex data processing and analysis tasks without any human intervention, which reduces the workload on employees so they can use their manpower on more strategic tasks. In addition, with AI teams can strategize operational workflow through automation. The biggest advantage of AI Cloud Computing is its ability to help small and large-scale companies streamline Big Data management without breaking the bank. Paired with Edge Computing, AI Cloud Computing helps companies develop advanced solutions that readily respond to customer requests while analyzing huge data flows that hide valuable business insights.

Critique

Network Connectivity

Cloud-based Machine Learning applications require consistent network connectivity sLack of connectivity can seriously hinder the processes that run on ML algorithms. Additionally, it takes time for the data to reach the cloud where it can be further processed There is a huge time lag between sending data to the cloud, which impacts prompt response and quick actions necessary for resolution.

Data Privacy

Another important challenge with AI Cloud Computing is data privacy. Is data privacy. The information collected through AI sensors captures both customer and vendor data before it is transferred and processed. Lack of security protocols in both web and mobile Cloud Computing can lead to data hacks that may lead to further security issues

Conclusion

In conclusion, cloud computing is recently new technological development that has the potential to have a great impact on the world. It has many benefits that it provides to it users and businesses. It reduces operating cost by spending less on maintenance and software upgrades and focus more on the businesses it self.

Concentrating on a case study set in a smart campus scenario. We discussed security issues such as data privacy, access control, and data availability. The lack of security measures and ease of access in the cloud can result in the compromise of data without the victim's knowledge. Hence, it is emphasized to deploy the efficient security and privacy measures to ensure data integrity, privacy, and reliability. However, cloud service providers are not providing enough security to satisfy users. Additionally, blockchain improves security problems in cloud computing.

It was observed from the study that data will keep on increasing as the year run by so it is important to know how to secure such vital information. Cloud environment is widely used in industry and research aspects; therefore security is an important aspect for organizations running on these cloud environments considering the fact that the best place to keep such big data is in the cloud.

The concept of cloud computing can be effectively used in the field of supply chain management facilitating mainly the collaboration among the supply chain stakeholders. More specifically, forecasting on the cloud can reduce the distortion of demand when moving away from the real customer's demand. Finally, subsequent academic research could possibly develop new advanced integrated cloud models for supply chain management, which will encourage the majority of companies.

Artificial Intelligence has been nothing but a miracle for humanity. From its inception to its current growth, AI applications have aided humanity in building better applications that predict, measure, and help us solve critical and complex problems. With AI Cloud Computing, the scope of those applications have expanded to offer even more flexibility and agility required for long-term growth in any sector