VAISHNAVI P SHET
4NM21CS199, TASK2

Examine the latest developments in secure and scalable cloud computing infrastructure, focusing on its role in supporting modern applications and businesses.

1. Cloud Computing: Security Issues and Research Challenges

[Journal of Network Communications and Emerging Technologies (JNCET) 2017
Moulika Bollinadi, Vijay Kumar Damera]

ABSTRACT:

Cloud Computing is a type of internet-based computing which provides services via the internet and accesses the resources within the user enterprise either in a private-own-cloud or on a third-party server On Demand. The model is characterized by three attributes: scalability, pay-per-use, self-services. Many industries such as banking, healthcare, Retail, Education, Manufacturing and business are adopting this cloud technique due to efficiency of services provided by pay-per-use pattern which helps in accessing the networks, storage, servers, services and applications, without physically acquiring them [3]. The circumscribed control over the data may cause various security issues in cloud computing like Data crash, Misuse and reprehensible use of cloud computing, Insecure API, Wicked Insiders, Shared technology issues/multi-tendency nature, Account services and Traffic Hijacking. There are many new technologies, improvements and research proceedings happening every day in order to develop the security and to provide assurance for users [2]. This research paper brings a framework on what cloud computing is, main security risks and issues that are currently present in the field of cloud computing, research challenges, importance in key industries and also the personal hypothesis on future advances in the field of cloud security.

SUMMARY:

This paper discusses the emergence of cloud computing as a transformative force in the realm of information technology. Cloud computing is a paradigm of solutions that has gained popularity due to its features such as scalability, pay-per-use, and self-

services. It has been widely adopted across various industries, including banking, healthcare, retail, education, and manufacturing. The impact of cloud computing on these industries, particularly in terms of data storage, access, and reliability, has been substantial. The three primary service models of cloud computing, namely Software as a Service (S-a-a-S), Infrastructure as a Service (I-a-a-S), and Platform as a Service (P-a-a-S), have played a pivotal role in reshaping the IT landscape. However, the widespread adoption of cloud computing has also brought about significant security concerns. This paper delves into the various security challenges associated with cloud computing, including data breaches, system vulnerabilities, account hijacking, and multi-tenancy effects. It emphasizes the need to address threats such as confidentiality, integrity, availability, and accountability in order to ensure the security and reliability of cloud-based services. Furthermore, the document highlights the rapid growth of cloud computing and the increasing adoption of internet and cloud-based services. It underscores the importance of developing new security technologies and enhancing existing ones to align with the architecture of cloud computing. The future of cloud computing is expected to involve advancements in automation, artificial intelligence (AI), and machine learning (ML), which may lead to a decrease in traditional programming jobs. The paper also discusses the potential research challenges and advancements in cloud security, emphasizing the need for continuous innovation and development in this field.

In conclusion, this paper provides a comprehensive overview of cloud computing, its impact on industries, security challenges, and potential research advancements. It underscores the critical role of cloud computing in shaping the future of the software industry and emphasizes the need for robust security measures to address the evolving threats in the digital landscape.

CONCLUSION:

Cloud Computing is an emerging technology with a concept of distributed computing. Though it has not come into a full force at present, the future of the software industry is completely going to be dependent on this concept. In this paper, we first discussed about what cloud computing is and Different services provided by Cloud. Later, Importance of cloud computing in key industries, Security issues and research

challenges, Applications of cloud computing and future advancements in cloud computing technology. We have observed that here are several security challenges including security aspects of network and virtualization. This paper has highlighted all the security issues in cloud computing and possibly how to avoid them too. New security technologies must be developed and older technologies are needed to be radically tweaked to be able to work with cloud architecture. We believe that Industries are the main sectors for usage of cloud services. The cloud usage in five key industries is studied in this report along with the increase in cloud usage from 2015 to 2017. Last but not least, as whole IT industry is looking forward for the process of Automation, we have provided an overview of how it is going to be with our imagination and what are the basic security issues that are going to be faced in the future. As Automation in Cloud Computing is still an ideal process which needs more clarity and research to be done, we hope that our work will provide a better understanding of design challenges in cloud computing and pave the path for future research in this area.

2. DATA SECURITY IN CLOUD COMPUTING

[Journal of Emerging Technologies and Innovative Research (JETIR) 2019
R. Sangeetha, M. Silambarasi]

ABSTRACT:

Cloud computing is a model which enables widespread access to a shared pool of resources including the characteristics of scalability, virtualization and many others. The most important service offered by cloud is storage wherein the users store the required data. Security is a concern here as the data is stored on remote server with multi user capabilities. The data is at the risk of unauthorized access thereby reducing reliability and privacy. The key issue in cloud regarding security is the openness of the host or service providers. A gateway to the hacker is being provided when a test environment is set on a cloud. Cloud allows exchange of information among its services which requires standards. This development of standards is tough due to the interoperability issues. An intruder can provide malicious threat to the cloud data. The developments of standards are still a concern in security of the cloud. Though there is

increasing research done to enhance the security, new issue arises, or the security method becomes inappropriate for the scalable services. Program clustering and slicing for user efficiencies is difficult for the same reason. To enhance the issues of cloud security such as • Data privacy. • Data integrity. • Prevent unauthorized access to the cloud. Managing interoperability. Keywords- Data security, Privacy protection, Cloud Computing.

SUMMARY:

This paper delves into the realm of cloud computing, highlighting its significance as a cost-effective and flexible platform for delivering IT services over the Internet. It emphasizes the need to address security concerns in cloud computing, particularly focusing on aspects such as data privacy, data integrity, and preventing unauthorized access. The risks associated with virtualization and storage in public cloud environments are underscored, emphasizing the necessity for careful risk management strategies to mitigate potential vulnerabilities. Furthermore, the paper delves into the various encryption techniques employed to safeguard data in the cloud. It discusses the utilization of block ciphers, stream ciphers, and hash functions as essential tools for protecting data integrity and confidentiality. The importance of access control, multi-tenancy, and threat identification in securing data within cloud environments is also emphasized, shedding light on the multifaceted nature of cloud security. Moreover, the paper highlights the differences in encryption techniques for data at rest and data in transit, emphasizing the criticality of their proper usage to ensure robust security measures. It provides insights into the complexities and nuances of securing data in cloud environments, offering a comprehensive overview of the security challenges and solutions within the realm of cloud computing.

In conclusion, this paper serves as a valuable resource for understanding the intricacies of cloud security, providing a holistic perspective on the complexities involved in safeguarding data within cloud environments. It offers a comprehensive analysis of the security challenges and solutions in cloud computing, shedding light on the multifaceted nature of securing data in the cloud and the critical importance of implementing robust security measures to protect sensitive information.

CONCLUSION:

Everyone wants to use the cloud for cost savings and for new business models. But for cloud security, it is very important to understand the different threats that come into play, says Derek Tumulak. Cloud is a promising technology for the future IT applications. The main requirement of an organization was reducing data storage and processing cost. The analysis of data and information are the most important tasks in all organizations to make the decisions. So, they will not be transferred by organization to the cloud till there is a trust between the cloud service providers and consumers. One of the major concerns of this paper was data security and its threats, and solutions in cloud computing. Data in different states have been discussed along with the techniques which are efficient for encrypting the data in the cloud. The study provided an overview of block cipher, stream cipher and hash function which are used for encrypting the data in the cloud whether it is at rest or in transit.

3. CSPCR: Cloud Security, Privacy and Compliance Readiness - A Trustworthy Framework

[International Journal of Electrical and Computer Engineering (IJECE) 2018
Sugandh Bhatia, Jyoteesh Malhotra]

ABSTRACT:

The privacy, handling, management and security of information in a cloud environment are complex and tedious tasks to achieve. With minimum investment and reduced cost of operations an organization can avail and apply the benefits of cloud computing into its business. This computing paradigm is based upon a pay as per your usage model. Moreover, security, privacy, compliance, risk management and service level agreement are critical issues in cloud computing environment. In fact, there is dire need of a model which can tackle and handle all the security and privacy issues. Therefore, we suggest a CSPCR model for evaluating the preparation of an organization to handle or to counter the threats, hazards in cloud computing environment. CSPCR discusses rules and regulations which are considered as pre-requisites in migrating or shifting to cloud computing services.

SUMMARY:

The document underscores the critical importance of information privacy and security readiness for organizations contemplating a shift to cloud computing services. It introduces the Cloud Security, Privacy, and Compliance Readiness (CSPCR) model, designed to assess the readiness of organizations in four major components: distribution of data, analysis of current policies, revamping and documentation of cloud information, and assessment of preparedness for cloud hazards. The study also sheds light on the availability of infrastructure in various countries to support the digital economy and cloud computing services. It emphasizes the need for training personnel, particularly security experts in management, and the utilization of Byzantine fault-tolerant service in the system.

Furthermore, the document outlines the feasibility study for CSPCR migration, encompassing economic and technical feasibility. It presents the CSPCR readiness model and references other relevant studies and frameworks. Additionally, the document delves into the importance of a policy framework for security and the creation of readiness in the system for enforcing policy in cloud information security and privacy. It also emphasizes the development of a cloud security policy along with a readiness framework as a crucial step in determining the necessary arrangements for security and privacy.

The document concludes by discussing the importance of integrity as a mechanism to ensure the consistency and accuracy of data available in the system during its lifecycle, and the control of Byzantine failures with the help of Byzantine fault-tolerant service in the system. It also highlights the significance of evaluating the readiness of the system, focusing on readiness analysis and feasibility study as crucial factors in the transformation of the cloud system. The migration plan should be reviewed by technical experts to ensure that all CSPCR requirements are in order prior to implementation.

CONCLUSION:

Nowadays, Government, private and non-government organizations are thinking to shift or has migrated to the cloud services due to myriad benefits of cloud computing

services. As a result, cloud security, privacy and compliance readiness and control have mutated as a prominent research area in the field of computing and information science. The present paper suggests a cloud security, privacy and compliance readiness model that performs a significant role to achieve the upgraded level of security. This readiness model is multi-dimensional and multi layered. It includes a hexagonal security model for analysing the various domains of cloud information security, privacy and compliance readiness requirements. The CSPCR model can be used to evaluate existing information security, privacy and compliance readiness. The proposed framework determines the organization attitude regarding the managing, controlling, operating, availability, compliant and secure cloud computing services. Moreover, the performance and ability of the technical personnel in the organization can be checked. According to this framework, a special concentration is devoted on organizing workshops, seminars and other activities to uplift the skills, education and awareness in the technical personnel of the organization. The CSPCR model is not designed only for the organizations planning migrate to cloud, but can also be executed to make any improvement in the system. The model can also be used as an optimization tool for the organizations that have implemented the cloud services and creates hazard aware and control environment which applauds prescient and sagacious operations in the system. Hence, this model helps an organization to evaluate any cloud services issues like security, privacy, compliance readiness and compatibility.