ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.9, 6577–6588
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.9.15 Spec. Issue on CAMM-2020

A STUDY OF RECENT ISSUES IN CLOUD COMPUTING TECHNIQUES

AMANPREET SINGH[1], AMANDEEP KAUR[2], DEEPALI GUPTA[3], NEHA GUPTA[4], AND KAMALI GUPTA[5]

ABSTRACT. Cloud computing plays a vital role in reducing the cost of hardware, software, infrastructure, platform, and other network items. An example of such cost saving in a typical organisation is, reduction of about 30% operational cost in online services by using cloud computing. Hence, a pay per use model can be adopted for deriving cost efficiency. This study presents an overview of a distributed system, cloud computing, virtualization and zookeeper. However, there have been various issues in cloud computing like data security, network security, data locality, data integrity, data segregation, authentication, authorization, access control, availability and backup. We conclude this paper with the challenges associated with cloud-based security, resource constraints, governance, and performance.

1. INTRODUCTION

Cloud computing is a channel to access computing resources through the Internet. It consists of hardware, networks and services that can be provided to users located anywhere in the world. Cloud computing offers its users, the advantage of low costs, location and device independence over traditional computing systems [1]. For end-user, the overall cost of hardware and other resources gets reduced because everything is located remotely, but providing maximum

[2]*corresponding author*

2010 *Mathematics Subject Classification.* 68W99, 70C20, 74-02.

Key words and phrases. Cloud Computing, Distributed System, Security, Virtualization, ZooKeeper.

output with minimum investment to the user [2]. Cloud Computing is a way of storing information in a data centre. According to David Patterson in 2008, "The data centre is the computer". However, recently according to Rajkumar Buyya of Melbourne University "The Cloud is the computer" [3]. Cloud computing, was preceded by a distributed computing system, as shown in Figure 1. However, in this era of evolution, the concept of cloud is proliferating in all directions.

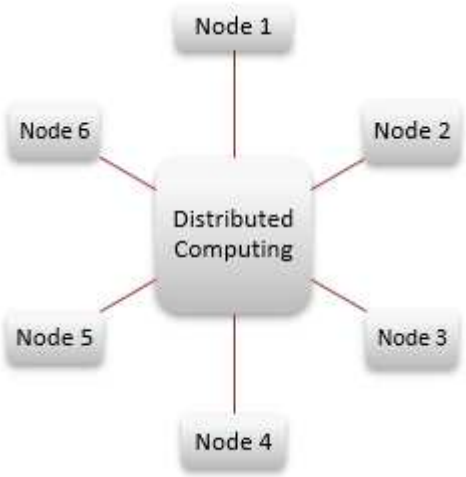

FIGURE 1. Distributed Computing System [2]

In the concept of cloud, the data is stored either in a physical or a virtual resource. Therefore cloud computer is also called utility computer.

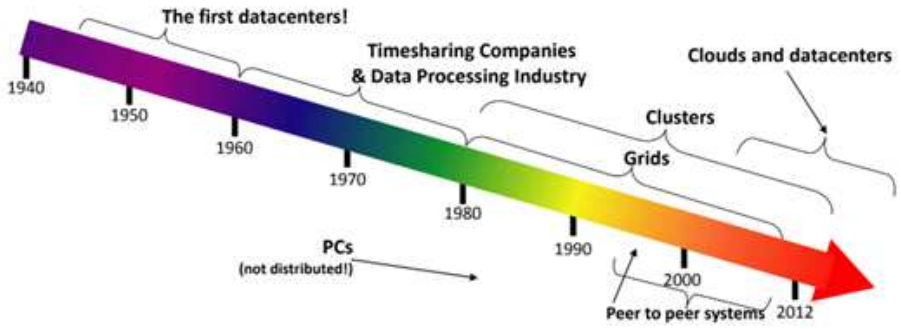

FIGURE 2. Cloud Computing and Distributed System [2]

As shown in Figure 2, during the period from 1940 to 1960, the data used to be stored in a data centre. Thereafter for the next two decades, time-sharing companies and the data processing industry took over data storage. Between 1980 to 2000, several companies like IBM, Xerox, Honeywell were leading the data storage market. From 2000 onwards, data is being stored in cloud and data centres.

2. LITERATURE REVIEW

The author discusses Virtualization, ZooKeeper, peer to peer in cloud computing during literature review.

2.1. **Virtualization in Cloud Computing.** Virtualization originated during the late 60s at IBM. Virtualization allows simultaneous execution of various operating systems and their applications on the identical real machine.

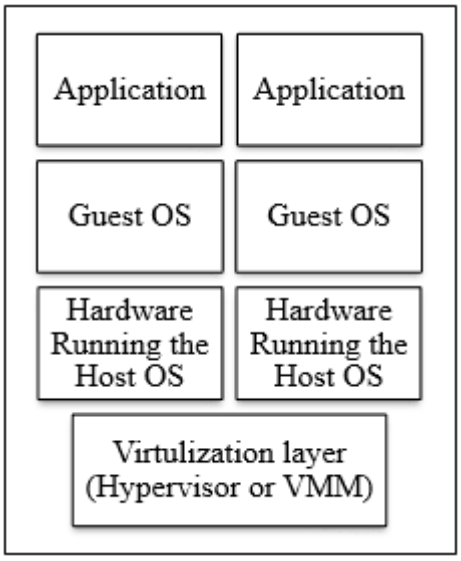

FIGURE 3. Virtualization in Cloud [4]

As shown in Figure 3, there is central hardware comprising the CPU, memory disk and other peripherals. This hardware when used by more than one application with its corresponding operating systems, then such sharing of a single resource with several individual isolated resources or environments is called as virtualization. Users can use the system as a separate individual physical resource. In such an arrangement, a single physical machine has multiple virtual

machines. Virtual machine means an operating system i.e. an application, and its virtual resources together. Here each operating system believes that it owns the entire hardware resources. The various hardware resources are known as the guest operating system, and many of such guest operating systems can reside separately and execute concurrently. As the physical resources are shared, these are called as virtual resources. These several operating systems access the same piece of hardware. The guest operating system can either own/use the entire resource or some part of the resource, available on the physical machine.

These several operating systems access the same piece of hardware. The guest operating system can either own/use the entire resource or some part of the resource, available on the physical machine. This setup requires the virtualization layer, also called as the operating system of several operating systems. The required operating system will provide the physical resources to be shared across multiple operating systems.

The virtualization layer is also called a hypervisor or virtual machine monitor (VMM). This hypervisor will manage the physical hardware resources to provide the virtualized view to several operating systems, called as guest operating systems. The virtual machine (VM) is the effective abstraction of the replica of the actual machine. Cloud computing heavily depends on server virtualization because of the sharing of physical infrastructure. A virtual machine allows multiplexing of hardware to hundreds of VMs connected the same physical server. Therefore, if multiple VM are spanning on the same physical machine, the problem is that they are quickly deployed whenever a new service is available [5].

Virtualization environment is classified into six categories, as shown in Figure 4. These are Distribution pattern-based, Scheduling-based, Energy-aware-based, Load distribution based, Operational-based and Transactional-based. Virtualization requires computing resources to duplicate certain computer resources [4].

2.2. **ZooKeeper as a distributed application in Cloud.** Zookeeper is a replicated service, which holds the metadata of the distributed applications. Zookeeper provides simple primitives, which are easy to program for the clients to use for their applications. It uses a simple data model like a directory tree or a directory structure of a file system. In distributed applications, zookeeper is used for synchronization. It is used for locking the consistency and maintaining the

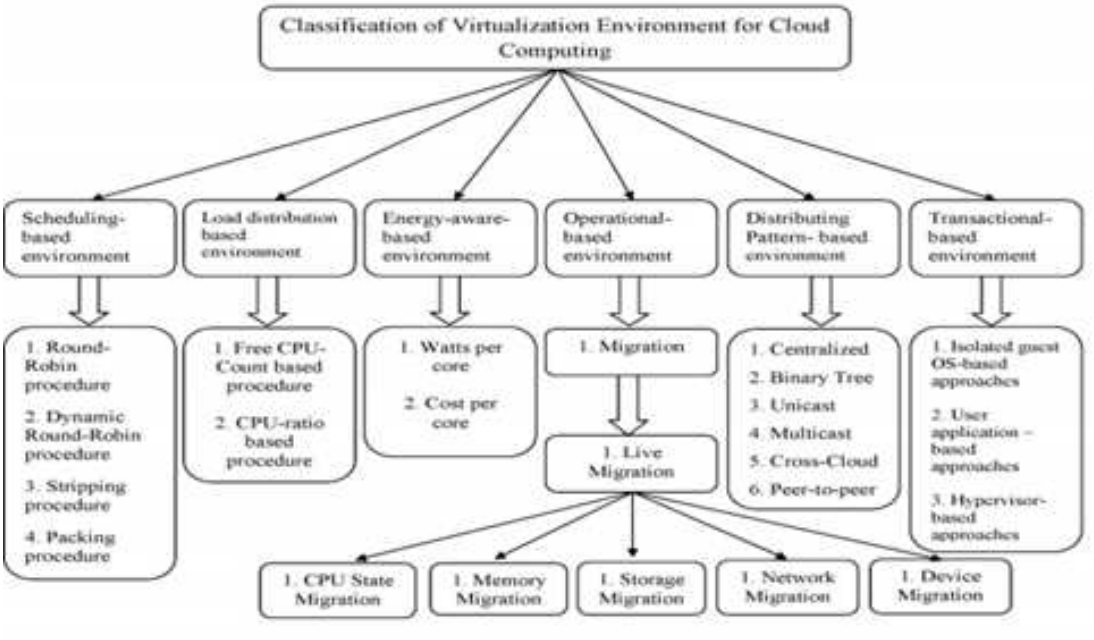

FIGURE 4. Classification of Virtualization Environment [4]

configuration, i.e. dynamic configuration and is therefore called distributed-locking. Such a coordination service, provided by the zookeeper ensures that it does not suffer from errors such as race conditions and deadlocks. ZooKeeper and Consul are fundamental building blocks for cloud applications [6]. Multiple processes running on multiple machines need central coordination. This central storage, which is responsible for the coordination, for all concurrent related issues, serves this purpose in the distributed system model. This central storage can be modelled as the zookeeper application. Zookeeper achieves running per second throughput for read-workloads using quick read with watches that are both critical for synchronization in various distributed applications [6].

2.3. **Peer to Peer Systems in Cloud Computing.** Distributed systems focus on scalability with the number of nodes. This is one of the primary issues, when the system is required to support many clients [7]. A highly scalable, large-scale distribution system is required to support many clients. One such system widely being accepted is called peer to peer system. The techniques of peer to peer system currently applied in various cloud computing systems such as key-value stores are, Cassandra, Riak, Voldemort. The system uses the chord peer to peer

systems like consistent hashing and virtual ring. There are widely deployed peer to peer systems like Napster, Gnutella, Fasttrack, and BitTorrent. Peer to peer systems came out from academia with all proven properties such as Chord, Pastry, and Kelips [7].

2.4. **Various challenges in cloud computing.** In the past decade, the use of cloud computing has changed the idea of how organizations operate. Cloud computing guarantees that companies can obtain and control their IT requirements quickly and cost effectively.

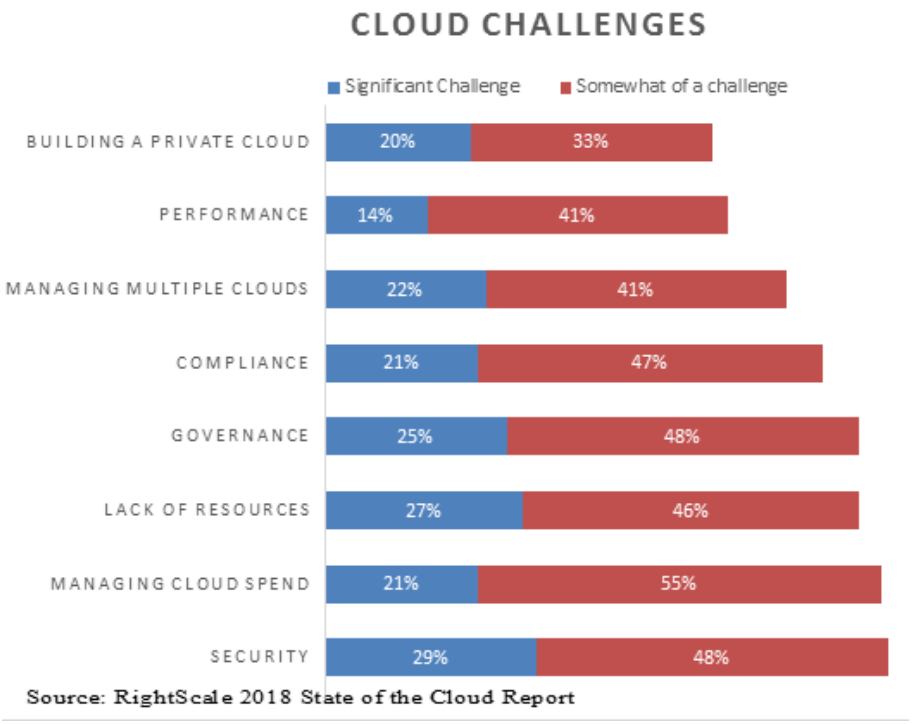

FIGURE 5. Cloud Challenges [2]

RightScale carried out the global State of the Cloud report on the new technology patterns in January 2018. 997 technology experts from a wide variety of organizations were asked regarding their implementation of cloud computing [2]. The findings were understandable, particularly about current cloud computing challenges. Following are some results and specific cloud infrastructure issues for organizations to resolve the critical issue of increasing cloud computing barriers it faces.

3. SECTION

3.1. **Security.** Cloud computing allows companies to focus on their core activities to increase their productivity. Cloud computing is referred to as the 'fifth utility' whereby computing services are available on-demand, just like all other utility services like water, energy, gas and telecommunications are available in society today. The performance and operation of tasks allocated over the resources raise specific security issues. These are service security and data security. The safety of data includes integrity, safeguarding against threats, privacy and cyber-attacks. The safety of services includes security of resources and confidentiality. Specific problems and protection boundaries must be addressed to accomplish an efficient resource schedule, including data security and accessibility [2]. Systematic Literature Review offers a standardized approach to methods and thorough interpretation of the state-of-the-art data management work [2]. Table 1 demonstrates the major security problems for each service model [9].

TABLE 1. Security Issues in various service models [9]

Security Issues	Service Models			Responsibility	
	IaaS	PaaS	SaaS	Sources	User
Data Security	Y	Y	Y	Y	
Network Security	Y	Y	Y	Y	
Data Locality	Y		Y	Y	
Data Integrity		Y	Y	Y	
Data Access	Y	Y	Y	Y	Y
Authorisation, Authentication	Y		Y	Y	
Data Confidentiality			Y	Y	
Availability	Y	Y	Y	Y	
Backup			Y	Y	Y
Identity Management	Y		Y	Y	

In data security, the data owner predefines the expected release period. A consumer cannot access any details until the period is specified. After the expiration time, a consumer cannot access any results. The confidential data will then be removed to maximize data protection after the expiration time. The period of authorization shall vary between the expected release time and the expiration time. Throughout the life cycle of the respective application, relevant consumer

data will be secured. A modern solution to solving cloud protection network issues can be introduced by the service function chain (SFC), which incorporates a software-defined network (SDN) and network function virtualization (NFV) [1]. In addition to the monetary costs charged from the end-users, the data location significantly impacts cloud performance, especially in terms of the percentage of SLA violations [8]. For making the data confidential, data must be encrypted before it is outsourced in order to protect against malicious internal or external attacks. Data integrity means protection from an illegal insertion, updation, or deletion and authorizing users to recognize if the data has been corrupted. SaaS has the most quality challenges, as it is more complicated than other versions. PaaS and IaaS have fewer security problems because of their better security control, and it does not participate in the application level. The providers are primarily responsible for ensuring the safety of the service. The problems of security in the service models, including networking security, make a considerable impact on the reliability, confidence, and security of each service model [9].

For deployment models like public, private, hybrid, and community: common safety issues are authentication, authorization, access control, availability and data security. Such safety issues are highly critical because the security level of each the implementation model is specific. Private, hybrid, and community clouds are more secure than public cloud. Malicious hackers are often aimed at collecting information which could then be used for private hacking. Service security is the responsibility of service providers, and any unauthorized access to the service must be prevented. Suspected behaviour includes any malicious attacks and device misconduct. Users too have responsibilities for the protection of information and data such as transparency, secrecy, authorization, and authentication.

The barriers encountering in cloud computing are summarized in Table 2 [10]. Armbrust et al. [10] suggests that consideration for each problem varies from one participant to another. Service availability with several sides is the first obstacle. On the one hand, cloud providers offer multiple services to maximize capacity, but users can choose to use more than one service. Therefore, certain portions of the infrastructure can be indefinitely inaccessible to some customers. There are many reasons for not providing services, such as crashing systems, heavy traffic loads, and server hijack [10]. The customers will then believe that the service was down and it is not safe for use. However, services

with multiple clouds provide a threat to the security from a hacker. An attacker can access resources using a public service without authorization or carry out a range of malicious activities that influences services. The use of a fast scale-up method and safety monitoring is a way to defend this problem [10]. Cloud scale approach, involves both horizontal and vertical scaling styles, and are used for managing cloud services [10]. Vertical or scale-up is used to increase the performance of Internet infrastructure, often referred to as outward spreading. The availability of services is a problem which can be resolved if this approach is not allowed for virtual resources.

Table 2: Obstacles and Category in Cloud [10]

Barriers	**Listing**	**Participant Prospective**
Service Support	Cloud Service Availability	End User
Data Reposting	Processed Information, Data limits	Supplier
Data hiding	Processed Information, Data limits	End User
Transferring of Data	Processed Information, Data limits	End User
Performance Uncertainty	Fulfilment, Flexibility	End User
Extensible Storage	Fulfilment, Flexibility	End User
Error of extensive scale	Fulfilment, Flexibility	Supplier
Quick Escalate	Fulfilment, Flexibility	End User
Service Level Agreement (SLA)	Service Plans	Supplier, End User
Software certificate	Service Plans	Supplier, End User

The next three barriers of data limits between platforms are, data reposting, data hiding, and transferring of data. Other security implications for consideration include data loss, information theft, data transfer, and data security. Performance Uncertainty, extensible storage, the error of extensive scale, quick escalate barriers are more technological in performance. Extensive storage, error elimination in a broad distribution network and the rapid development of scalable networks provide a summary of operating costs. Quick Escalate may render the service inaccessible if the safety consequences of this approach involve high load tasks. The ninth and tenth barriers are services level agreement

(SLA) and software certificate. These are necessary to ensure that the software used is authorized and the license is not misused [10].

3.2. **Cost management and containment.** Any organization can make a profit through a cloud because of having no need to buy new hardware for processing the data. As the cloud services are on-demand, businesses run smoothly by using (pay-as-you-go) PAYG cloud computing.

3.3. **Lack of resources.** The lack of resources for businesses is a problem for the cloud. Various user organizations upload their valid data in the cloud. Cloud technologies are changing very fast; therefore, it becomes difficult to maintain compatibility between the cloud technologies and resources of various organizations.

3.4. **Governance/Control.** Cloud computing is faced with many challenges. The objectives of the business are to strictly follow laid down policies and to implement all the IT assets in compliance to the rules of IT governance. Timely maintenance for the upkeep of the assets to deliver its rated performance efficiently is to be achieved, recorded and presented/published.

3.5. **Controlling multiple clouds.** Cloud infrastructure problems were not centralized in one area. In recent years, the prominence of multi-cloud has grown exponentially. 81% of businesses in a study had a multi-cloud approach. In 2017, public and private-cloud combined software firms, dropped from 58 to 51 percent, while companies with a multi-state cloud strategy or several private clouds increased slightly.

4. OTHER EXISTING WORK IN CLOUD FROM PERIOD 2009 TO 2020 YEAR

Year of Publication	**Summary**
2009	Previously, 61% of companies used public clouds, 38% used proprietary clouds and 29% used hybrid clouds [3].

2009	The life cycle of implementation is certainly changing with the emergence of social networks and cloud computing. This is because social networks go beyond the life cycle and cloud computing often cuts and changes life-cycle activities [10].
2013	Cloud computing is "A model for providing convenient, on-demand network access to a common bundle of configurable computing resources which can be delivered and released quickly with minimal management effort or service provider interactions [4]".
2017	Helps promote greater interest in IS research (information systems) and organizes research efforts in this important sector through the proposed IS efficiency framework for non-profit organizations [8].
2019	In 39 papers, the SLR (systematic literature review) approach has been used to determine the status of cloud-based adoption by SMEs, hypotheses employed, advantages and challenges faced by SMEs [2].
2020	The content analysis results, showed cloud computing trends and patterns during 2009-2014, with a view to enhance cloud computing's maturity. Several security concerns arise because of the sharing of cloud by various users [1].

5. CONCLUSION

A difference is observed between distributed and cloud computing systems. It is evident that the advantages of cloud computing outweigh its drawbacks and it is far more beneficial than the traditional distributed computing system. Consequently, the user base of cloud computing is constantly increasing. The services of cloud computing are IaaS, PaaS, and SaaS, which play a vital role in reducing operational and maintenance costs at the user end. Nowadays, along with IaaS, PaaS, and SaaS services, Everything as a Service (EaaS) is also being used in cloud computing. The cloud is being implemented using virtualization. Zookeeper plays a vital role in fundamental building blocks for cloud applications. Peer to peer system supports multiple clients. Cloud implementation has its own sets of issues/challenges like cost management, lack of resources, control, managing multiple clouds, and the biggest one being security. Data security is still the prime concern on the public cloud. Security implications include data loss, information theft, data transfer. Service availability on cloud is an equally important issue to be resolved.

REFERENCES

[1] J. LUO, S. YU, S. PENG.: *SDN/NFV-Based Security Service Function Tree for Cloud*, IEEE Access. **8** (2020), 38538–38545.

[2] A. SHEIKH, M. MUNRO, D. BUDGEN: *Systematic Literature Review (SLR) of Resource Scheduling and Security in Cloud Computing*, International Journal of Advanced Computer Science and Applications. **10**(4) (2019), 35–44.

[3] R. BUYYA, C.S. YEO, S. VENUGOPAL, J. BROBERG, I. BRANDIC: *Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility.*, Future Generation Computer Systems, **25**(2009), 599–616.

[4] P. SOUVIK, P.K. PATTNAIK: *Classification of virtualization environment for cloud computing*, Indian Journal of Science and Technology **6** (2013), 3965–3971.

[5] M. MERVE BAYRAMUSTA, V. ASLIHAN NASIR: *A fad or future of IT? A comprehensive literature review on the cloud computing research*, International Journal of Information Management, **36**(4) (2016), 635–644.

[6] S. BRENNER, C. WULF, D. GOLTZSCHE, N. WEICHBRODT, M. LORENZ, C. FETZER, P. PIETZUCH, R. KAPITZA: *SecureKeeper: Confidential ZooKeeper using Intel SGX*, In Proceedings of the 17th International Middleware Conference (Middleware '16). **Article 14**(2016), 1–13.

[7] R. MORENO-VOZMEDIANO, E. HUEDO, R. S. MONTERO, I. M. LLORENTE: *A Disaggregated Cloud Architecture for Edge Computing*, IEEE Internet Computing, **23**(3) (2019), 31–36.

[8] G. L. STAVRINIDES, H. D. KARATZA: *The impact of data locality on the performance of a SaaS cloud with real-time data-intensive applications*, Proc. - 2017 IEEE/ACM 21st Int. Symp. Distrib. Simul. Real Time Appl. DS-RT 2017, (2017), 1–8.

[9] S. SUBASHINI, V. KAVITHA: *A survey on security issues in service delivery models of cloud computing*, Journal of Network and Computer Applications, **34**(1) (2011), 1–11.

[10] FOX, A., GRIFFITH, R., JOSEPH, A., KATZ, R., KONWINSKI, A., LEE, G., ... & STOICA, I: *Above the clouds: A berkeley view of cloud computing*, Department Electrical Eng. and Comput. Sciences, University of California, Berkeley, **28**(13) (2009), 2009.

[1,2,3,4,5]DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, CHITKARA UNIVERSITY, PUNJAB, INDIA

Email address: [1]amanpreet.singh@chitkara.edu.in

Email address: [2]amandeep.bhullar@chitkara.edu.in

Email address: [3]deepali.gupta@chitkara.edu.in

Email address: [4]neha.gupta@chitkara.edu.in

Email address: [5]kamali.singla@chitkara.edu.in