A Secure and Synchronized Cloud Ecosystem for Students Academics and Professional Records

Hariom Kumar*, Rajkumar R**

* M.Sc Computer Science
** Prof SCSE VIT University, India

Abstract- Cloud computing refers to computing with a focus of virtualized computer networks or resources and application services by improving the utilization of data centre and data resources. In the existing system, it has been analyzed that the risks and availability of student's academic records and information are very likely to be centralized, static in nature and one time use only. The proposed system is based on cloud environment; it communicates as well as synchronized with different academic clouds and provides a way of freedom to students regarding their academics and professional achievements. In this paper we seek cloud computing environment as a new opportunity in deploying cloud based application for keeping academics and professional records of students and figure the academic cloud ecosystem and ensuring security and confidentiality for the data by using Randomized Alphanumeric Cipher (RAC) algorithm. This academic cloud ecosystem is going to define the shape of a new era record keeping place and will be available worldwide.

Index Terms- Cloud ecosystem, data centre, virtualization, RAC security, confidentiality.

I. INTRODUCTION

In today's world where technology has taken over all industries from automobile, food processing and even production houses, how the education system can remain untouched. In the absence of software, there are too many difficulties in keeping records manually. Records may be electronic or hard copy. This paper seeks to handle and keep all the student's academic records in cloud environment thus form academic cloud ecosystem. Hence resulting in better record keeping facility and efficient usage of time. Cloud Computing (CC) is an emerging sound technology with service on demand that is pay and use service in the ICT (Information and Communication Technology). It moves the application software and databases to the large data centers, and offers subscription-based access to infrastructure, platforms, and applications that are popularly known as IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service). While these emerging services have increased interoperability and usability and reduced the computation cost, hosting of application, and content storage and delivery by several orders of magnitude, there is significant complexity involved in ensuring that applications and services can scale as needed to achieve consistent and reliable operation under peak loads. Various IT vendors are promising to offer computation, storage, and application hosting services and to provide coverage in several continents with commitments and offering service-level agreements (SLA) performance and uptime promises for their services. While these clouds are the natural evolution of traditional data centers, they are distinguished by exposing resources computation, data-storage, and applications as standards-based web services and following a utility pricing model where customers are charged based on their utilization of computational resources, storage, and transfer of data commonly known as pay as peruse service. It is a key step in the development and deployment of virtualization of a great number of distributed applications over the computer networks or the internet. It allow us and business body to use cloud applications without installation and access the information at anytime anywhere on any computer with internet access. The CC is a culmination of numerous attempts at large scale computing with seamless access to virtually limitless resources. Entities for cloud services providers such as Amazon, Rackspace, IBM, and Microsoft all offer environments for developing and deploying applications in the cloud. CC comes with aim of distributed data centers' and data resources. Each concerned data centre is composed of physical machines to execute customer's request on virtual machines where applications are provided over the Internet through browser. These services may include compute, network, and storage components. Customers benefit by subscribing to cost-efficient resources on a service provider scale and obtaining increased agility and productivity. Some IaaS benefits includes: Consolidation through virtualization, Infrastructure amortization, Economic efficiencies, Opening of new markets, Differentiation from over-the-top providers. There is vast number of basic technologies, services, and infrastructure that compose cloud computing. In this era of modern society and increased techno trends in the information technology, information is provided to the concerned entities as upon their request. Students earn the academic credits during their academic session and they have the right to get their achievements anytime anywhere. Cloud computing ensures access to remote services with a user's data, software and computation. This paper is organized in this way; Section 1 Abstract and Introduction, Section 2 Related existing system. Section 3 Description of the proposed model along with its architecture description and performance analysis. Section 4 Conclusion and future work.

II. EXISTING SYSTEM

In recent years a variety of systems to facilitate Record Keeping has been developed. Although these systems typically have common goals. They aim at different fields of application and executing them.

Virtualization is one of the most important technologies among them. It is a mechanism of abstracting the hardware and system resources which are located remotely. It has revolutionized center of data technology with the help of a set of techniques and tools that facilitate the providing and management of the dynamic data center's infrastructure. It has become an essential and enabling technology of cloud computing environments. Virtualization can be defined as the abstraction of the four computing resources these are storage, processing power, memory, and network. Virtualization enables high, reliable, and agile deployment mechanisms and management of services, providing on-demand service and live migration services which improve reliability. Accordingly, having an effective management's suite for managing virtual machines infrastructure is critical for any cloud computing infrastructure as a service (IaaS) vendor. Many web sites and web services are available for record keeping for different –different types of information like banking, financial, educational etc.

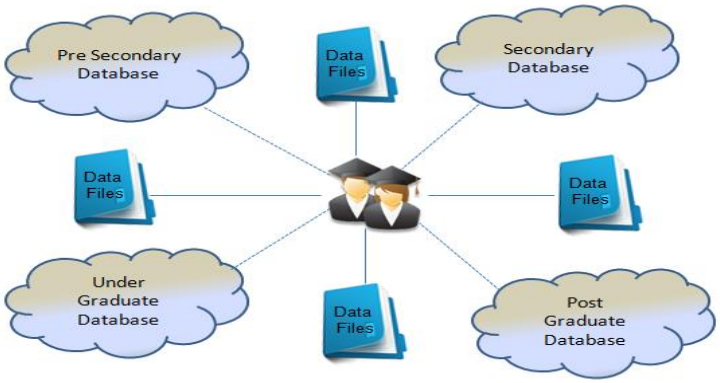

Fig:-1 Existing System for keeping student academic records.

In the existing system students academic records are kept in a hard copy file in the office of the institution which is issued by the authorized party. And same copy is also issued to the students in time only once after completion of his course. From fig:1-The solid lines indicate that a hard copy of student's records has been issued to the respective students whereas the dotted lines show that the academic information is also kept in electronic or digital form into the databases. This copy is used for many purposes like admission in college/university or for job interviews. Now for the job interviews or for the admission candidates move from place to place with original hard copy of the certificates and they have to take care of these wherever they go for counseling and interviews. But in this system disaster like lost of files during travelling, fire etc my happen any time. And to get back the lost file again though the system rules and regulations is very much time consuming even although the concerned institution issue the copy of the file which is equivalent to original files or certificates ,it get delay. By going through these system protocols to get back their academic records students can lose the opportunity to enroll in the college/University for higher studies or may be sometimes job.

III. PROPOSED SYSTEM

In this paper, a model is proposed for keeping student's academic records and achievements in secure and synchronized cloud environment which provides the facilities to the students to get their academic information anytime anywhere. As the system is digital and available over the network i.e. internet students don't have to worry about to carry hard copy of their original documents wherever they move , since these documents are their own academic assets they can access these whenever they need it that is service on demand. For a post graduate student he might be pursued his pre secondary, secondary and undergraduate diploma or degree from different board and university and all his records are kept separately to the institutions respectively and considered as different clouds. As cloud computing is achieving increased popularity, concerns are being expressed about the security issues introduced through adoption of new models. The effectiveness and efficiency of traditional protection mechanisms are being reconsidered as the characteristics of this innovative deployment model can differ widely from those of traditional architectures. An alternative perspective on the topic of cloud security is that this is but another, although quite broad, case of applied security and that similar security principles that apply in shared multi-user mainframe security models apply with cloud security. Here cloud made up of computers is extending beyond a single company or an enterprise. The applications and data served by the cloud are available to broad concerned group of users; it crosses enterprise and crossed the platform. Service is accessed via the Internet. Any authorized user can access these docs and apps from any computer over any internet connection. And, to the user, the technology and infrastructure behind the cloud is invisible. It isn't apparent and, in most cases it doesn't matter whether cloud services are based on HTTP, HTML, and XML, JavaScript, PHP or other specific technologies. In the proposed model I want to build a cloud ecosystem in which all the concerned board clouds and the institution clouds will we be synchronized and will communicate with each other based on the insolvent of student's identity. We will provide strong authentication and security ID to the student to log into the cloud ecosystem and to get their academic and achievements anytime anywhere.

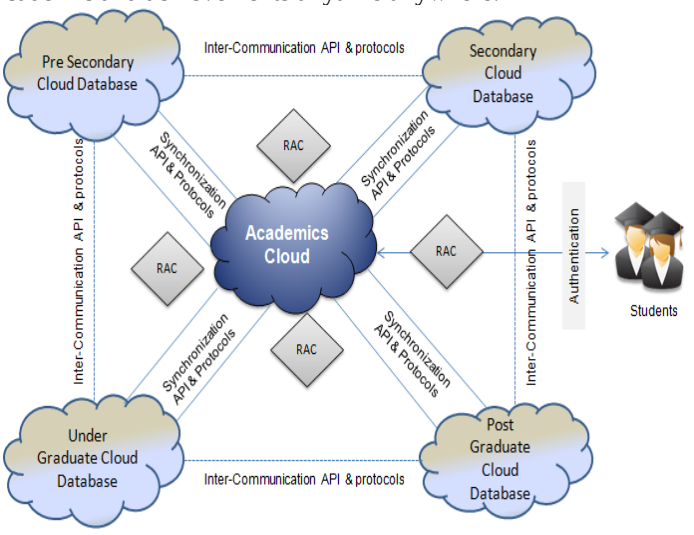

Fig:-2 Proposed Academic Cloud Ecosystem

Students are pursuing their courses during academic session in different intuitions and educational bodies and their academic records are issued to them as upon completion of courses. Here cloud made up of computers is extending beyond a single academic institution. The applications and data served by the cloud are available to broad concerned group of users that is student; Service is accessed via the Internet. Any authorized student can access these docs from any computer over any Internet connection. And, to the user, the technology and infrastructure behind the cloud is invisible. It isn't apparent and, in most cases it doesn't matter whether cloud services are based on HTTP, HTML, and XML, JavaScript, PHP or other specific technologies. In the proposed Academic Cloud Ecosystem the students' academic databases are intercommunicated with the help of proper protocols and APIs (Application Program Interfaces). Usage of the API is via the HTTP protocol. These APIs allows us to write portable code that can interoperate with multiple cloud vendors. The cloud API brings cloud technologies to PHP and the PHPilosophy to the cloud, starting with common interfaces for four cloud application services such as file storage, document storage, simple queues and infrastructure. It is cooperative effort of several major cloud vendors to create a single, simple, interoperable API that works with many cloud services and providers. This works under way to add support for more cloud services and cloud providers. Cloud computing won't reach its full potential without openness and flexibility. The simple cloud API is an important tool for keeping the cloud open and the applications flexible. For a post graduate student his/her academic records are distributed among different institutions; academic cloud ecosystem is synchronized among pre secondary database, secondary database, under-graduate database and post-graduate database via APIs and protocols. In other words, this cloud application can make use of these academic databases and services with no concern over how the application will be deployed. System is configured to maintain compatibility with services and academic databases; the data source can be chosen through configuration changes alone at the time of deployment. From Fig: 2 It would be visualized that student will be authenticated and get login to the Academic Cloud System with unique ID to view their profiles and academic details on a single click.

Security Concern for Authentication RAC (Randomized Alphanumeric Cipher) Algorithm

We provide authentication and security with the help of Randomized Alphanumeric Cipher (RAC) algorithm. It is based on asymmetric key cryptography and uses random functions with specific way of bit stuffing and stuffing.

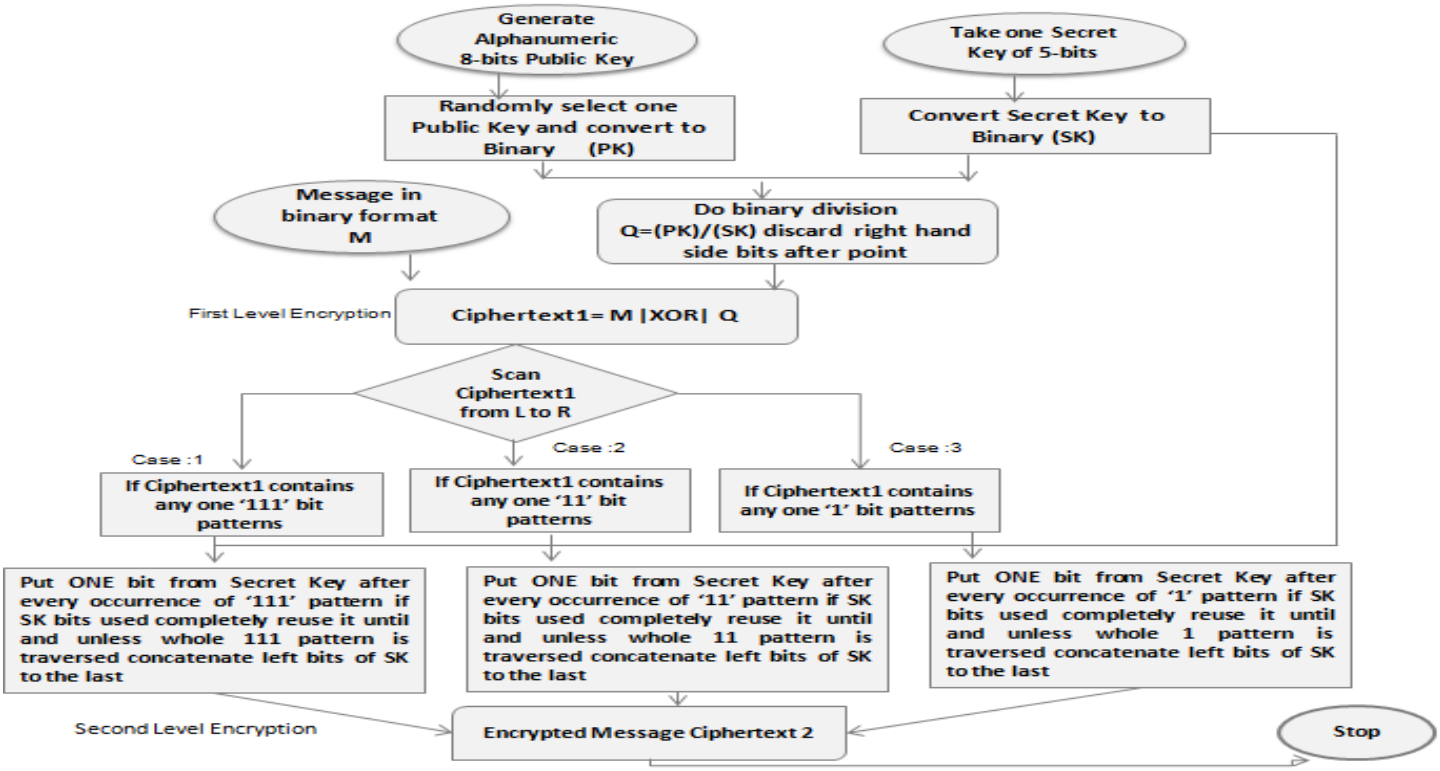

Fig:-3 Flowchart RAC algorithm

Encryption Algorithm

- Randomly generate N number of 8-bit alphanumeric characters.
- Select one public key (PK) of 8-bit and one secret key (SK) of 5-bits.
- Convert Public Key and Private Key to binary format.
- Compute the quotient of binary division where Q= (PK)/ (SK).
- Take message (M) and convert into binary format.
- Perform XOR operation with message 'M' and quotient 'Q'. It gives first level encryption Ciphertext1=M|XOR|Q
- Scan the Ciphertext1 from left to right as per cases mentioned in flowchart.
- Perform specific bit stuffing for particular selected case.
- Concatenate the unused bits of SK at last
- It results second level encryption and we get cipertext2

Decryption Algorithm

- It is just the reverse of Encryption.
- Remove the appended bits from ciphertext2.
- Remove stuffed bits and match it with SK bits. If removed bits equals with SK bits.
- We get ciphertext1.First level decryption over.
- Perform XOR with ciphertext1 and quotient Q.
- This results plain message 'M'. Second level of decryption.

.

RAC algorithm is used for encryption and decryption of students ID and provides strong authentication to login to academic cloud ecosystem.

Analysis

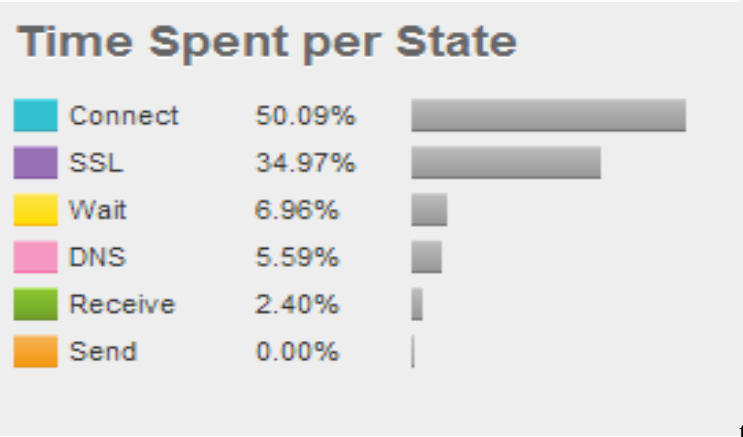

Fig:-4 Time Spent per state

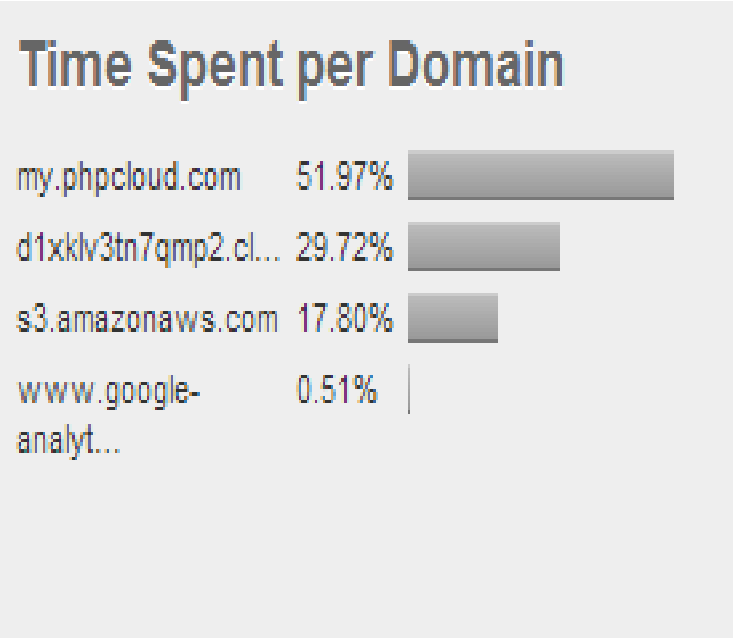

Fig:-5 Time Spent per Domain

Above diagram of fig-4 shows that time spent per state such as connection time, SSL (Secure Socket layer), Waiting time, DNS (Domain Name Server) time, receive time and send time.Fig-5 indicates comparatively time spent per domain like my.phpcloud.com,s3.amazonaws.com,google etc.

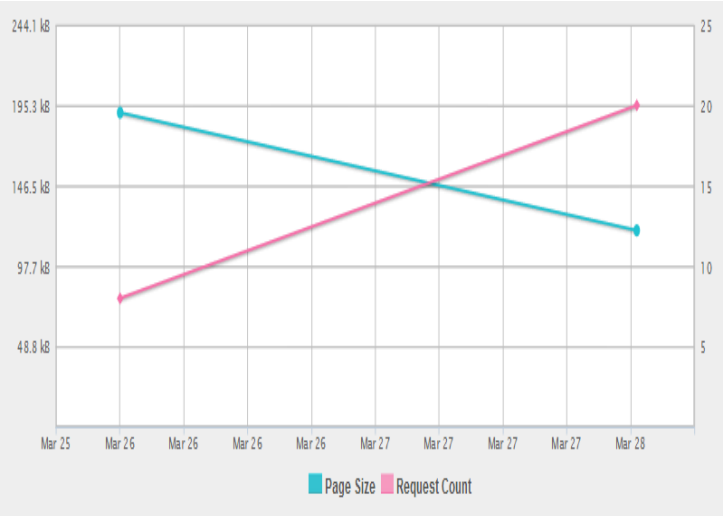

Fig:-6 Page Size and Request Count

Fig -6 shows that page size with respect to request count of that page throughout the user log session in academic cloud ecosystem.

IV. Conclusion & Future work

In this paper records keeping of 'students academic records and their achievements 'problem without the cloud computing has been studied and a modified cloud ecosystem for keeping the academic performance of the students is proposed with authentication and security assurance. The system will be reliable, available, synchronized, and communicatable and completely remove the fear of lose of files and the documents. This system will reduce the risks of lost of files. By using this model in future students can move to any city and any place for job interviews and for counseling for higher studies and his achievements are always with them. As applications software needs to both scale down rapidly as well as scale up, which is a new requirement for keeping the records. Such software also needs a pay-for-use licensing model to match needs of cloud ecosystem. Therefore, we tried to fix up the students record keeping which bring significant impact to their carrier and life. However, in the face of the significant benefits offered by cloud computing, the current technologies are not matured enough to recognize its full potential for record keeping. So many key challenges in this domain including automatic resource provisioning, power management and security management are starting to receive attention from the research community for the real world problems. This holds only as long as there are no appropriate service level agreements with upper boundaries between Cloud operators and users.

References

[1] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI, "Homomorphic Encryption Applied to the Cloud Computing Security", WCE 2012.

[2] Vic (J.R.) Winkler,"Securing the Cloud, Cloud Computer Security, Techniques and Tactics", Elsevier, 2011.

[3] Uma Somani, Kanika Lakhani, Manish Mundra" Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", IEEE, 2010.

[4] Huaglory Tianfield" Security Issues in Cloud Computing", IEEE, 2012.

[5] Wentao Liu" Research on Cloud Computing Security Problem and Strategy", IEEE, 2012.

[6] Amazon.com, "Amazon Web Services (AWS)," Online at http://aws.amazon.com, 2008.

[7] Cloud Security Alliance www.cloudsecurityalliance.org http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf /

[8] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, "The Eucalyptus Open-source Cloud-computingSystem," Proceedings of Cloud Computing and Its Applications, 2008.

[9] Meiko Jensen, Jorg Sehwenk et al., "On Technical Security, Issues in cloud Computing"IEEE International conference on cloud Computing, 2009

[10] Yubo Tan , Xinlei Wang "Research of Cloud Computing Data Security Technology"IEEE 2012

[11] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On Technical Security Issues in Cloud Computing," in Cloud Computing, 2009. CLOUD '09. IEEE International Conference on, 2009, pp. 109-116.

[12] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1",

Authors

First Author – Hariom Kumar , M.Sc (Computer Science), VIT University, Vellore, khariom58@yahoo.com

Second Author – Rajkumar R , Assistant Professor (Senior)-SCSE VIT University, Vellore, rrajkumar@vit.ac.in