A DESIGN AND DEVELOPMENT OF A MODEL TO AUTHORIZE CERTIFICATES IN GOVERNMENT SECTORS USING CLOUD COMPUTING ENVIRONMENTS

Yogeesh A.C[1], Roopashree H.R[2], Anjan punith B.G[3], Rajesh. B[4]
Assistant Professor, Department of Computer Science and Engineering[1], Senior TRM L[2], Sapient India pvt ltd[2], Under Graduate student, Department of Computer Science and Engineering[3], Under Graduate student, Department of Computer Science and Engineering[4], Government Engineering college, Kushalnagar-571234

Abstract

In this paper we have design and developed a model, where user can request and administrator can authorizes certificates through online in several sectors. we used fifth generation cloud computing environments to maintain data.This model enables a convenient, on-demand network access for a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort. we developed an application which allow users to make a request to get certificates (e.g Income/Residential/Land Records e.tc..) through online by filling user application form by attaching appropriate proof (voter id, Dl,Aadhar card,ration card e.t.c..).all this process will be carried out in main remote server which is placed in the public cloud and it can be accessible by all the web based systems through online on-demand. we also maintain a Private cloud in which special privileged administrator(i.e.village accountant and thashildar) authorize certificates(using digital signatures) by access/reviewing data from public cloud. We ensure the data Integrity and security using Rsvp security algorithm and enhance the applications search in public and private cloud using Cloudle search engine.

Keywords— Cloud Computing, Cloudle search engine, RSVP Security, Private Cloud, Public Cloud.

Introduction

This paper works on the basis of cloud computing [1], here the main remote server is placed in the public cloud which provides on-demand access for the users and special privileged administrators (i.e. village accountant and thashildar). Here the application is placed or installed in main server that can be access by the user through online by using website tools or web browsers. The cloud computing provides and deliver application via internet which are accessed from web browsers by using devices such as the laptop, desktop, mobile etc[2], while data is stored on the server at a remote location.

Cloud Architecture

Cloud architecture, the systems architecture of the software systems involved in the delivery of cloud computing, typically involves multiple cloud components communicating with each other over a loose coupling mechanism such as a messaging queue.[2]

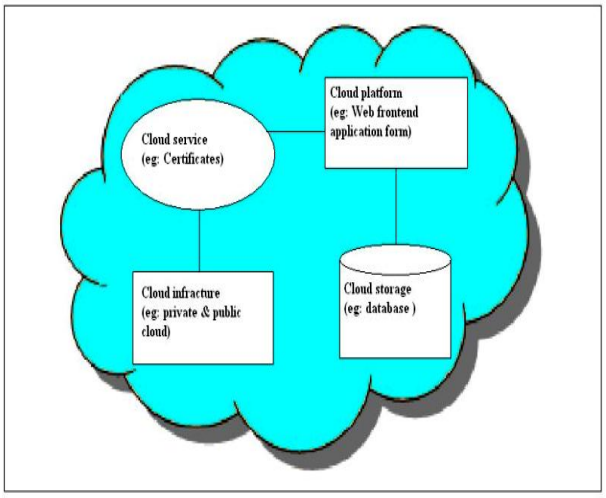


Figure 1: Cloud computing architecture to authorize certificates

***Cloud services*:** Cloud application services or "Software as a Service (SaaS)" deliver software as a service over the Internet, eliminating the need to install and run the application on the customer's own computers and simplifying maintenance and support, In this case we are providing the certificates(eg. Income tax, Ration card, Residential and RTC…)

Cloud platforms: Cloud platform services, also known as platform as a service (PaaS), deliver a computing platform and/or solution stack as a service, often consuming cloud infrastructure and sustaining cloud applications. It facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers. Cloud computing is becoming a major change

in our industry, and one of the most important parts of this change is the shift of cloud platforms. Platforms let developers write certain applications that can run in the cloud, or even use services provided by the cloud. There are different names being used for platforms which can include the on-demand platform, or Cloud 9. In our case we are providing the platform to the users by filling Application form which is available on internet. User can fill application form irrespective of understanding the underlying technology.

***Cloud Infrastructure*:** Cloud infrastructure services, also known as "infrastructure as a service" (IaaS), deliver computer infrastructure – typically a platform virtualization environment – as a service, along with raw (block) storage and networking. Rather than purchasing servers, software, data-center space or network equipment, clients instead buy those resources as a fully outsourced service. Our Cloud Infrastructure consist of Private and Public cloud and Providing security using RSVP security algorithm [4].

***Cloud Storage Server*:** The servers layer consists of computer hardware and/or computer software products that are specifically designed for the delivery of cloud services, including multi-core processors, cloud-specific operating systems and combined offering

Cloud Processing Stages to Authorize Certificates

This model uses cloud computing environment that works in five stages as follows:

***Stage 1*:** The main server is placed in the public cloud, which allows 'n' number of users to make request by filling user application form in order to get a certificates through online. They need to fill the required information in the form and have to attach a appropriate proof (voter id, Dl, Aadhar card, ration card) in the .jpeg or .jpg format, and upload in to the public cloud server by using any of the web browser that is available in the system through Internet, then the documents are verified and accepted by the particulars in by getting the data from public to private cloud to authorizes certificate. After some processes the particular user will get notification message, that message consists of unique identity code (e.g.:INCXXXXXX)[3][5] then they have to use their unique identity code for downloading the certificates.

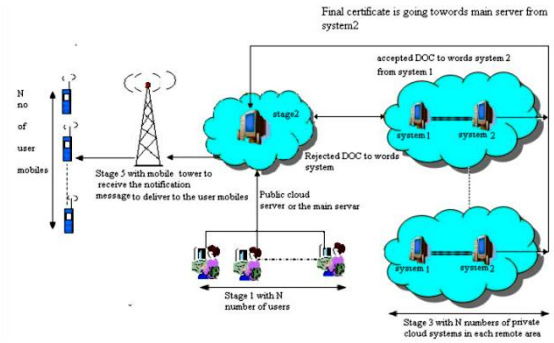


Figure 2: Development and design of entire processing stages to authorize certificates.

***Stage 2*:** The uploaded document of user is present in the main public cloud server, which consist of all the uploaded documents of the users through the internet. Once the document is uploaded to server it does not allow any users to modify the documents which have been uploaded. It allows only for accept or reject the uploaded document for a special privileged user who are operating in private cloud systems (i.e. village accountant of particular remote area) through their unique account. The public cloud server facilitates to send the notification massages to the users about their document progress.

Stage 3: There are n numbers of private cloud remote areas, each private cloud consist of two systems (i.e. village accountant system and thashildar system) in each private cloud remote area there are two special privileged users are present (i.e. village accountant and thashildar). Each privileged users have a unique account, through that they will be handling the public cloud server documents that belong to their particular area. The village accountant (system 1) after accessing to the public cloud server he/she looks for uploaded document in order to verify, if the document is correct then the village accountant prepares a new document called FINAL CERTIFICATE consisting of user name, address and all required data for the certificate then it sends to thashildar system (system 2) in order to get signed to the income certificate. If the uploaded document is not correct then it is rejected by the village accountant and he guides the public cloud server to send a notification message to particular user i.e. "Your uploaded document is incorrect, please provide correct proof".

Stage 4: In this stage the signed income certificate from the thashildar sends to the public cloud server and thashildar guides the public cloud server to send notification message to the particular user i.e. "Your income certificate is ready and collect by downloading in our website by providing this

unique identity code : INCXXXXXX. This income certificate is valid only for current year".

***Stage 5*:** In this stage the all notification messages from the public cloud server will be delivered to mobile tower then that message will be delivered to particular users mobile and the users also allowed replying their feedback.

Cloud Search Engine

In this paper, we are using search engine for Cloud computing system (Cloudle)[5] to search applications effectively by users and authorizing persons. Cloudle which is Cloud service search engine as the one of application using Cloud ontology. Users can sepecify application ID and Date of Birth for searching the application and authorizing persons can serach application by using the application id and DOB is not necessary.

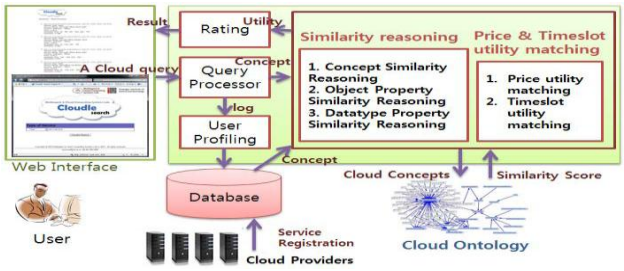


Figure 3: Cloudle system architecture

Cloudle system runs as follows. At first, users send queries(here Application id and DOB) to the Cloudle system through a web interface Also Cloud providers register their Cloud services into database of Cloudle. After that, the service discovery agent carries out five functionalities: (1) Query processing, (2) User profiling, (3) Similarity reasoning, (4) Price and timeslot utilities matching and (5) Rating.

Scope & Control Between Cloud Subscriber & Cloud Provider

Figure 4 illustrates the differences in scope and control between the cloud subscriber and cloud provider, for each of the service models discussed above. Five conceptual layers of a generalized cloud environment are identified in the center diagram and apply to public clouds, as well as each of the other deployment models. The arrows at the left and right of the diagram denote the approximate range of the cloud provider's and user's scope and control over the cloud environment for each service model. In general, the higher the level of support available from a cloud provider, the more narrow the scope and control the cloud subscriber has over the system.

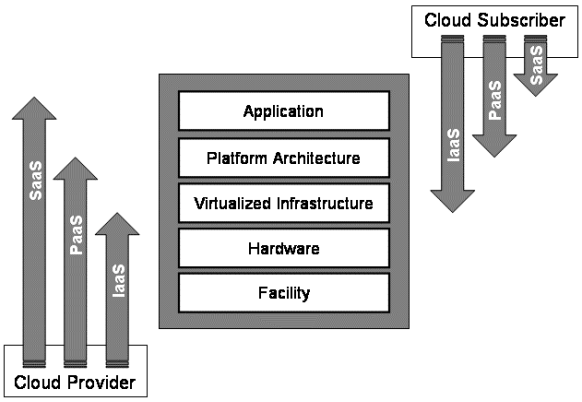


Figure 4: Differences in Scope and Control among Cloud Service Models

The two lowest layers shown denote the physical elements of a cloud environment, which are under the full control of the cloud provider, regardless of the service model. Heating, ventilation, air conditioning (HVAC), power, communications, and other aspects of the physical plant comprise the lowest layer, the facility layer, while computers, network and storage components, and other physical computing infrastructure elements comprise the hardware layer.

The remaining layers denote the logical elements of a cloud environment. The virtualized infrastructure layer entails software elements, such as hypervisors, virtual machines, virtual data storage, and supporting middleware components used to realize the infrastructure upon which a computing platform can be established. While virtual machine technology is commonly used at this layer, other means of providing the necessary software abstractions are not precluded.

Similarly, the platform architecture layer entails compilers, libraries, utilities, and other software tools and development environments needed to implement applications. The application layer represents deployed software applications targeted towards end-user software clients or other programs, and made available via the cloud. Some have argued that the distinction between IaaS and PaaS is fuzzy, and in many commercial offerings, the two are more alike than different [Arm10]. Nevertheless, these terms do serve a purpose, distinguishing between very basic support environments and environments having greater levels of support, and accordingly different allocations of control and responsibility between the cloud subscriber and the cloud provider. While cloud computing can be implemented exclusively for an organization as a private internal cloud, its main thrust has been to provide a vehicle for outsourcing parts of that environment to an outside party as a public cloud. As with

any outsourcing of information technology services, concerns exist about the implications for computer security and privacy. The main issue centers on the risks associated with moving important applications or data from within the confines of the organization's computing center to that of another organization (i.e., a public cloud), which is readily accessible by the general public.

Reducing cost and increasing efficiency are primary motivations for moving towards a public cloud, but reducing responsibility for security should not be. Ultimately, the organization is accountable for the overall security of the outsourced service. Monitoring and addressing security issues that arise remain in the purview of the organization, as does oversight over other important issues such as performance and availability. Because cloud computing brings with it new security challenges, it is essential for an organization to oversee and manage how the cloud provider secures and maintains the computing environment and ensures data is kept secure.

Public Cloud Services

The Security Upside

While the biggest obstacle facing public cloud computing is security, the cloud computing paradigm provides opportunities for innovation in provisioning security services that hold the prospect of improving the overall security of some organizations. The biggest beneficiaries are likely to be smaller organizations that have limited numbers of information technology administrators and security personnel, and lack the economies of scale available to larger organizations with sizeable data centers. Potential areas of improvement where organizations may derive security benefits from transitioning to a public cloud computing environment include the following:[7]

Staff Specialization

Cloud providers, just as organizations with large-scale computing facilities, have an opportunity for staff to specialize in security, privacy, and other areas of high interest and concern to the organization. Increases in the scale of computing induce specialization, which in turn allows security staff to shed other duties and concentrate exclusively on security issues. Through increased specialization, there is an opportunity for staff members gain in-depth experience, take remedial actions, and make security improvements more readily than otherwise would be possible with a diverse set of duties.

Platform Strength

The structure of cloud computing platforms is typically more uniform than that of most traditional computing centers. Greater uniformity and homogeneity facilitate platform hardening and enable better automation of security management activities like configuration control, vulnerability testing, security audits, and security patching of platform components. Information assurance and security response activities also profit from a uniform, homogeneous cloud infrastructure, as do system management activities, such as fault management, load balancing, and system maintenance. Many cloud providers meet standards for operational compliance and certification in areas like healthcare (e.g., Health Insurance Portability and Accountability9 Act (HIPAA)), finance (e.g., Payment Card Industry Data Security Standard (PCI DSS)) and audit (e.g., Statement on Auditing Standards No. 70 (SAS 70)).

Resource Availability

The scalability of cloud computing facilities allows for greater availability. Redundancy and disaster recovery capabilities are built into cloud computing environments and on-demand resource capacity can be used for better resilience when facing increased service demands or distributed denial of service attacks, and for quicker recovery from serious incidents. When an incident occurs, an opportunity also exists to capture information more readily, with greater detail and less impact on production. In some cases, however, such resiliency can have a downside. For example, an unsuccessful distributed denial of service attack can quickly consume large amounts of resources to defend against and cause charges to soar, inflicting serious financial damage to an organization.

Backup and Recovery

The backup and recovery policies and procedures of a cloud service may be superior to those of the organization and, if copies are maintained in diverse geographic locations, may be more robust. Data maintained within a cloud can be more available, faster to restore, and more reliable in many circumstances than that maintained in a traditional data center. Under such conditions, cloud services could also serve as a means for offsite backup storage for an organization's data center, in lieu of more traditional tape-based offsite storage. However, network performance over the Inter-

net and the amount of data involved are limiting factors that can affect restoration.

Mobile Endpoints

The architecture of a cloud solution extends to the client at the service endpoint, used to access hosted applications. Cloud clients can be browser-based or applications-based. Since the main computational resources needed are held by the cloud provider, clients are generally lightweight computationally and easily supported on laptops, notebooks, and netbooks, as well as embedded devices such as smart phones, tablets, and personal digital assistants.

Data Concentration

Data maintained and processed in the cloud can present less of a risk to an organization with a mobile workforce than having that data dispersed on portable computers or removable media out in the field, where theft and loss of devices routinely occur. Many organizations have already made the transition to support access to organizational data from mobile devices to improve workflow management and gain other operational efficiencies. Besides providing a computing platform or substitute for in-house applications, public cloud services, such as the following, can also be focused on provisioning security to other computing environments.

Data Center Oriented

Cloud services can be used to improve the security of data centers. For example, electronic mail can be redirected to a cloud provider via mail exchange (MX) records, examined and analyzed collectively with similar transactions from other data centers to discover widespread spam, phishing, and malware campaigns, and to carry out remedial action (e.g., quarantining suspect messages and content) more comprehensively than a single organization would be able to do. Researchers have also successfully demonstrated a system architecture for provisioning cloud-based antivirusservices, as an alternative to host-based antivirus solutions.

Cloud Oriented

Cloud services are available to improve the security of other cloud environments. For example, reverse proxy products are available that enable unfettered access to a SaaS environment, yet maintain the data stored in that environment in encrypted form . Cloud-based identity management services also exist, which can be used to augment or replace an organization's directory service for identification and authentication of users to a cloud.

The Security Downside

Besides its many potential benefits for security and privacy, public cloud computing also brings with it potential areas of concern, when compared with computing environments found in traditional data centers. Some of the more fundamental concerns include the following:[7]

System Complexity

A public cloud computing environment is extremely complex compared with that of a traditional data center. Many components comprise a public cloud, resulting in a large attack surface. Besides components for general computing, such as deployed applications, virtual machine monitors, guest virtual machines, data storage, and supporting middleware, there are also components that comprise the management backplane, such as those for self-service, resource metering, quota management, data replication and recovery, workload management, and cloud bursting. Cloud services themselves may also be realized through nesting and layering with services from other cloud providers. Components change over time as upgrades and feature improvements occur, confounding matters further. Security depends not only on the the correctness and effectiveness of many components, but also on the interactions among them. The number of possible interactions between components increases as the square of the number of components, which pushes the level of complexity upward. Complexity typically relates inversely to security, with greater complexity giving rise to vulnerabilities.

Shared Multi-tenant Environment

Public cloud services offered by providers have a serious underlying complication—subscribing organizations typically share components and resources with other subscribers that are unknown to them. Threats to network and computing infrastructures continue to increase each year and have become more sophisticated. Having to share an infrastructure with unknown outside parties can be a major drawback for some applications and requires a high level of assurance for the strength of the security mechanisms used for logical separation. While not unique to cloud computing, logical separation is a non-trivial problem that is exacerbated by the scale of cloud computing. Access to organizational data and resources could inadvertently be exposed to other subscribers through a configuration or software error. An attacker

could also pose as a subscriber to exploit vulnerabilities from within the cloud environment to gain unauthorized access.

Internet-facing Services

Public cloud services are delivered over the Internet, exposing both the administrative interfaces used to self-service an account and the interfaces for users and applications to access other available services. Applications and data that were previously accessed from the confines an organization's intranet, but moved to the cloud, must now face increased risk from network threats that were previously defended against at the perimeter of the organization's intranet and from new threats that target the exposed interfaces. The effect is somewhat analogous to the inclusion of wireless access points into an organization's intranet at the onset of that technology. Requiring remote administrative access as the sole means to manage the assets of the organization held by the cloud provider also increases risk, compared with a traditional data center, where administrative access to platforms can be restricted to direct or internal connections.

Loss of Control

While security and privacy concerns in cloud computing services are similar to those of traditional non-cloud services, they are amplified by external control over organizational assets and the potential for mismanagement of those assets. Migrating to a public cloud requires a transfer of control to the cloud provider over information as well as system components that were previously under the organization's direct control. Loss of control over both the physical and logical aspects of the system and data diminishes the organization's ability to maintain situational awareness, weigh alternatives, set priorities, and effect changes in security and privacy that are in the best interest of the organization. As with any technology, cloud computing services can be turned towards improper or illicit activities. A couple of noteworthy instances have already occurred that give a sense of what might be expected in the future.

Botnets

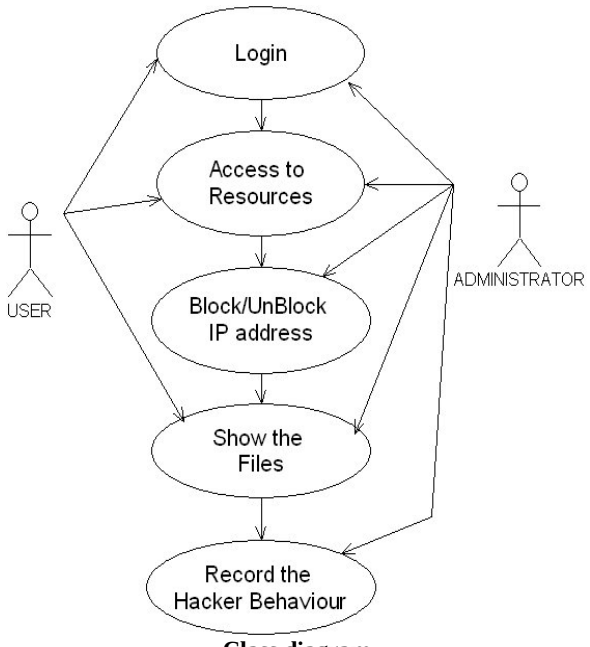
In many ways, botnets assembled and controlled by hackers are an early form of cloud computing. Cost reduction, dynamic provisioning, redundancy, security, and many other characteristics of cloud computing apply. Botnets have been used for sending spam, harvesting login credentials, and launching injection attacks against Websites . Botnets could be used to launch a denial of service attack against the infrastructure of a cloud provider. The possibility that a cloud service could become infiltrated by a botnet has already occurred; in 2009, a command-and-control node was12 discovered operating from within an IaaS cloud [Mcm09a, Whi09]. Spammers have also purchased cloud services directly and launched phishing campaigns, ensnaring recipients with malware via social engineering techniques.

Mechanism Cracking

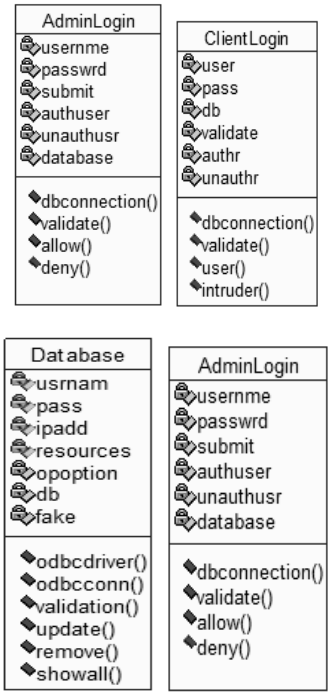
WiFi Protected Access (WPA) Cracker, a cloud service ostensibly for penetration testers, is an example of harnessing cloud resources on demand to determine the encrypted password used to protect a wireless network. With cloud computing, a task that would take five days to run on a single computer takes only 20 minutes to accomplish on a cluster of 400 virtual machines [Rag09]. Because cryptography is used widely in authentication, data confidentiality and integrity, and other security mechanisms, these mechanisms become, in effect, less effective with the availability of cryptographic key cracking cloud services. Both cloud-based and traditional types of systems are possible targets. CAPTCHA cracking is another area where cloud services could be applied to bypass verification meant to thwart abusive use of internet services by automated softwares .

Use Case Diagram's

A use-case diagram is a graph of actors, a set of use cases enclosed by a system boundary, participation associations between the actors and the use-cases, and generalization among the use cases. In general, the *use-case* defines the outside (actors) and inside(use-case) of the system's typical behavior. A use-case is shown as an ellipse containing the name of the use-case and is initiated by actors. An *Actor* is anything that interacts with a use-case. This is symbolized by a stick figure with the name of the actor below the figure.



Class diagram



Conclusion and Future Work

This application reduces time to get certificates and allows access them from anytime, anywhere through Internet. Users can able access through any web based tools(web browsers) and requires only minimum knowledge of internet, user can easily download or collect Approved authorized certificates through online/office. It overcome the traditional way of getting certificates by standing in queue, running from one offices to other to get signatures and mainly corruption in government sectors. It also environmental friendly as it reduces the papers usage and also replication of certificates is very easy. We can enhance this application by adding good mathematical model, algorithms and web rich application tools for increasing efficiency of time, space complexity of processing applications and good looking of user interface design [6].

Acknowledgment

This work was supported by teaching staff of Department of computer science and engineering, Government engineering college Kushalanagar, Karnataka.

References

[1] Cloud Computing: The Fifth generation of Computing. IEEE 2011 International Conference on Communication Systems and Network Technologies, Sameer Rajan Apurva Jairath Govt.of India, MCIT, DIT Department. Of C.S. & Engg. National Informatics Centre (NIC) G.G.I.T.S.Naharlagun, Arunachal Pradesh (India) Jabalpur M.P. (India).

[2] Mobile Cloud Computing Service Based on Heterogeneous Wireless and Mobile P2P Networks [3] Bernd Mohr, Computational Yanuarius Teofilus Larosa_, Jiann-Liang Chen_, Der-Jiunn Dengy, and Han-Chieh Chaoz_Department of Electrical Engineering, National Taiwan University of Science and Technology.

[3] Cloud computing - Wikipedia, the free encyclopedia

[4] Alberto leon-garcia communication networks, fundamental concepts and key architecture second edition.

[5] Ontology and Search Engine for Cloud Computing System, Proceedings of 2011 International Conference on System Science and Engineering, Macau, China - June 2011.

[6] 1st international IEEE workshop on collaboration and computing, Creating Next Generation Cloud Computing based Network Services and The Contributions of Social Cloud Operation Support System (OSS) to Society - Miyuki Sato, Fujitsu Co. Ltd, Japan

[7] Guidelines on Security and Privacy in Public Cloud Computing . NIST, National institute of standard & technology , US department of commerce by Wayne Jansen, Timothy Grance .

Yogeesh A.C obtained his Bachelor of Engineering in Computer Science from R.L Jalappa Institute of Technology and Master of Technology in Computer science and engineering from M.V Jayaraman College of engineering, Bangalore. He is currently working as a Assistant Professor, Department of Computer Science and Engineering, Government Engineering College, Kushalnagar, Kodagu, Karnataka, India. His areas of interest are Cloud Computing, Data Mining and Digital Image Processing.

Roopashre H.R obtained her M.Tech (Computer science and engineering) from Visvesvaraya Technological University, Belagum.Karnataka, India. She is currently working as Senior TRM L1 at sapient India pvt ltd. Her areas of interests are Cloud computing, VLSI and Embedded systems

Anjan punith B.G studying in final year Bachelor of Engineering, Department of Computer science and engineering, Government Engineering College Kushalnagar, Kodagu, Karnataka, India.. His areas of interest are Cloud Computing, Artificial Intelligence ,web designing , Space research & agriculture .

Rajesh.B, studying in final year Bachelor of Engineering, Department of Computer science and engineering, Government Engineering College Kushalnagar, Kodagu, Karnataka, India.. His areas of interest are Cloud Computing, UI development & core java .