ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

A Novel Method for Storage Security in Cloud Computing

D. Kanchana, Dr. S. Dhandapani

Abstract*— Cloud computing is a model for delivering information technology services in which resources are retrieved from the internet through web-based tools and applications, rather than a direct connection to a server. Data and software packages are stored in servers. However, cloud computing structure allows access to information as long as an electronic device has access to the web. This paper studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, consider the task of allowing a third party auditor, on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The support for data dynamics via the most general forms of data operation, such as block modification, insertion, and deletion, is also a significant step toward practicality, since services in Cloud Computing are not limited to archive or backup data only. In particular, to achieve efficient data dynamics, to improve the existing proof of storage models by manipulating the classic Merkle Hash Tree construction for block tag authentication. Extensive security and performance analysis show that the proposed schemes are highly efficient and provably secure.

***Index Terms*—Authentication, Cloud Computing, Data Integrity, Storage Security.**

I. INTRODUCTION

Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth. The concept of cloud computing model [1] is shown in Fig. 1.

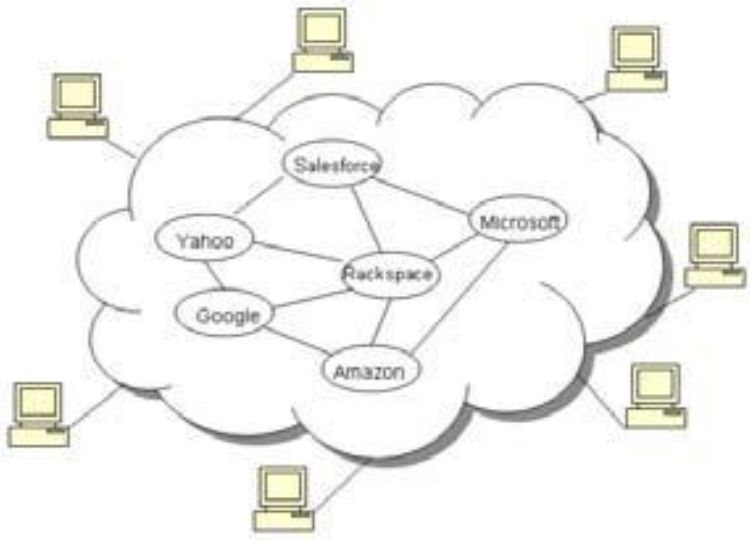

Fig. 1 Cloud Computing

The concept of cloud computing represents a shift in thought, in those end users need not know the details of a specific technology. The service is fully managed by the provider. Users can consume services at a rate that is set by their particular needs. This on demand service can be provided at any time.

II. RELATED WORK

A. Literature Survey

In order to solve this problem, many schemes are proposed under different systems and security models. In all these works, great efforts are made to design solutions that meet various requirements: high scheme efficiency,

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013
stateless verification, unbounded use of queries and retrieve ability of data, etc. Considering the role of the verifier in the model, all the schemes presented before fall into two categories: private verifiability and public verifiability. Although schemes with private verifiability can achieve higher scheme efficiency, public verifiability allows anyone, not just the client (data owner), to challenge the cloud server for correctness of data storage while keeping no private information [2].

Then, clients are able to delegate the evaluation of the service performance to an independent third party auditor (TPA), without devotion of their computation resources. In the cloud, the clients themselves are unreliable or cannot afford the overhead of performing frequent integrity checks [3]. Thus, for practical use, it seems more rational to equip the verification protocol with public verifiability, which is expected to play a more important role in achieving economies of scale for Cloud Computing. That is, the outsourced data themselves should not be required by the verifier for the verification purpose [4].

To consider the problem of efficiently proving the integrity of data stored at untrusted servers. In the provable data possession (PDP) model, the client preprocesses the data and then sends it to an untrusted server for storage, while keeping a small amount of meta-data [5]. The client later asks the server to prove that the stored data has not been tampered with or deleted (without downloading the actual data). However, the original PDP (provable data possession) scheme applies only to static (or append-only) files.

B. Secure Architecture Models

Open Security Architecture (OSA) provides free frameworks that are easily integrated in applications, for the security architecture community. Its patterns are based on schematics that show the information traffic flow for a particular implementation as well as policies implemented at each step for security reasons [6].

The following description of a proposed cloud computing architecture, also shown in Figure.2.2, should help the reader envision the components of cloud computing architectures along with descriptions of elements that make it secure [7]. The important entities involved in the data flow are end users, developers, system architect, 3rd party auditors and the cloud itself.

C. End Users

End Users need to access certain resources in the cloud and should be aware of access agreements such as acceptable use or conflict of interest. In this model, end user signatures may be used to confirm someone is committed to such policies [8]. The client organization should run mechanisms to detect vulnerable code or protocols at entry points such as firewalls, servers, or mobile devices and upload patches on the local systems as soon as they are found. Thus, this approach ensures security on the end users and on the cloud alike [3]. However, the cloud needs to be secure from any user with malicious intent that may attempt to gain access to information or shut down a service. For this reason, the cloud should include a denial of service (DOS) protection [9].One way of enforcing DOS protection is done by improving the infrastructure with more bandwidth and better computational power which the cloud has abundantly. However, in the more traditional sense, it involves filtering certain packets that have similar IP source addresses or server requests. The next issue concerning the cloud provider to end users is transmission integrity [10]. One way of implementing integrity is by using secure socket layer (SSL) or transport layer security (TLS) to ensure that the sessions are not being altered by a man in the middle attack. At a lower level, the network can be made secure by the use of secure internet protocol (IPsec). Lastly, the final middle point between end users and the cloud is transmission confidentiality or the guarantee that no one is listening on the conversation between authenticated users and the cloud. The same mechanisms mentioned above can also guarantee confidentiality.

D. System Architects

System architects are employed with writing the policies that pertain to the installation and configuration of hardware components such as firewalls, servers, routers, and software such as operating systems, thin clients, etc. They designate control protocols to direct the information flow within the cloud such as router update/queuing protocols, proxy server configurations or encrypted tunnels [11].

E. Developers

Developers building an application in the cloud need to access the infrastructure where the development environment is located. They also need to access some configuration server that allows them to test applications from various views. Cloud computing can improve software development by scaling the software environment through elasticity of resources. For example, one developer can get extra hard space as an on-demand resource, instead of placing a work order and wait for several days for the permission. Developers may desire extra virtual machines to either generate test data or to perform data analysis, processes which take significant time [12].

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

Also, using more processing power from the cloud can help in catching up with the development schedule. The cloud also helps developers create multiple evaluation versions environments for their applications, bypassing the need to incorporate additional security within the application and placing the burden on the cloud provider.

One significant drawback of cloud computing at the moment is its limitations to Intel x86 processor architecture. Even if this may very well change in the future, it is another stumbling block that developers and cloud computing experts need to overcome. Software monitoring may be done by monitoring API calls for server requests. With an architectural model where data is centralized, all eyes are focused in one direction, which implies better monitoring, although ultimately the issue rests with the developers/clients on how much effort will be directed in this regard. As far as security patches for the software as service approach, updating a patch is easier done in the cloud and shared with everyone seamlessly, rather than finding every machine that has the software installed locally.

F. Third Party Auditors

Third party auditors (TPA) are used by clients and providers alike to determine the security of the cloud implementation. Depending on the level of commitment to security and usefulness in obtaining a competitive edge, a cloud vendor may choose to submit itself to regular security assessments in an attempt to obtain accreditation. The accreditation process needs to be undertaken every three years. Thus, in order to lower the constraints on the cloud vendor, some organizations may implement continuous monitoring of the cloud system.

G. Overview

The cloud is the resource that incorporates routers, firewalls, gateway, proxy and storage servers. The interaction among these entities needs to occur in a secure fashion [13]. For this reason, the cloud, just like any data center, implements a boundary protection also known as the demilitarized zone (DMZ). The most sensitive information is stored behind the DMZ. Other policies that run in the cloud are resource priority and application partitioning. Resource priority allows processes or hardware requests in a higher priority queue to be serviced first. Application partitioning refers to the usage of one server or storage device for various clients that may have data encrypted differently. The cloud should have policies that divide the users' view of one application from the backend information storage. This may be solved by using virtualization, multiple processors or network adaptors.

III. METHODOLOGY

Cloud computing is the long dreamed vision of computing as a utility, where data owners can remotely store their data in the cloud to enjoy on-demand high-quality applications and services from a shared pool of configurable computing resources. While data outsourcing relieves the owners of the burden of local data storage and maintenance, it also eliminates their physical control of storage dependability and security, which traditionally has been expected by both enterprises and individuals with high service-level requirements.

In order to facilitate rapid deployment of cloud data storage service and regain security assurances with outsourced data dependability, efficient methods that enable on-demand data correctness verification on behalf of cloud data owners have to be designed. In this research to propose that publicly auditable cloud data storage is able to help this nascent cloud economy become fully established. With public audit ability, a trusted entity with expertise and capabilities of data owners do not possess can be delegated as an external audit party to assess the risk of outsourced data when needed [14]. Such an auditing service not only helps save data owners computation resources but also provides a transparent yet cost-effective method for data owners to gain trust in the cloud. To describe the approaches and system requirements that should be brought into consideration, and outline challenges that need to be resolved for such publicly auditable secure cloud storage service to become a reality. Cloud architecture [15] is shown in Fig. 2.

A. Network Methodology

The Network Methodology of this thesis is:

- Authentication module
- Web server identification
- Encryption
- Web server updation
- Decryption
- Data verification

Authentication Module

This module is to register the new users and previously registered users can enter into the project. The Register user only can enter into Proposed Process in the Project.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

Web Server Identification

The available Peer List is obtained by entering the workgroup name. This peer list is divided into active peer list and inactive peer list. The active peer list is divided into long lived peer and short lived peer. The long lived peer list is selected and is used for further process.

Encryption

Encryption is used to securely transmit data in open networks. Data encryption needs to be secure by resisting statistical attacks and other types of attacks. In this module data encrypted in the use of key and stored in TPA part.

Web Server Updation

In this module the original data stored in a particular selected web server .web server used for user processing. User can able to process these data without rules.

Decryption

Decryption is the reverse process to Encryption. Frequently, the same Cipher is used for both Encryption and Decryption. While Encryption creates a Cipher text from a Plaintext, Decryption creates a Plaintext from a Cipher text. In this module decrypt the encrypted information for verification

Data Verification

In this module data verification performed in the use of already decrypted content with old content. In this verification used to identify the changes in web server data

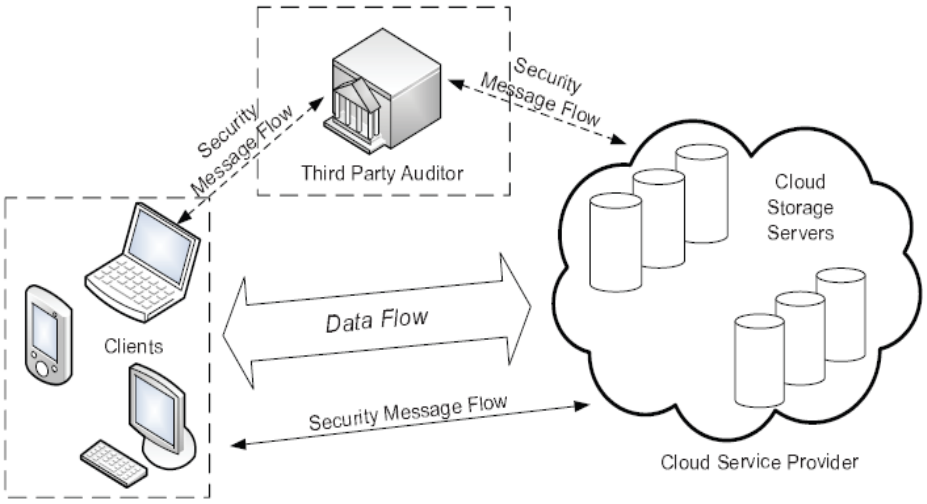

Fig. 2 Cloud Architecture

B. Implementation

Cloud computing makes these advantages more appealing than ever, it also brings new and challenging security threats to the outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing actually relinquishes the owner's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is put at risk due to the following reasons [16]. Hence, to fully ensure data security and save data owners' computation resources, to propose to enable publicly auditable cloud storage services, where data owners can resort to an external TPA to verify the outsourced data when needed. Third party auditing provides a transparent yet cost-effective method for establishing trust between data owner and cloud server. In a word, enabling public risk auditing protocols will play an important role for this nascent cloud economy to become fully established; where data owners will need ways to assess risk and gain trust in the cloud.

C. Maintenance

The reason that linear combination of sampled blocks may potentially reveal owner data information is due to the following fact about basic linear algebra theory: if enough linear combinations of the same blocks are collected, the TPA can simply derive the sampled data content by solving a system of linear equations. Exploiting data encryption before outsourcing is one way to mitigate this privacy concern, but it is only complementary to the privacy-preserving public auditing scheme to be deployed in cloud [17]. Without a properly designed auditing protocol, encryption itself cannot prevent data from flowing away toward external parties during the auditing process. Thus, it does not completely solve the problem of protecting data privacy but

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

just reduces it to the one of managing the encryption keys. Unauthorized data leakage still remains a problem due to the potential exposure of encryption keys. This way, the linear combination of sampled blocks in the server's response is masked with randomness generated by the server [18].

D. Design Methodologies

The data design transforms the information domain model created during analysis into the data structures that will be required to implement the software. The data objects and relationships defined in the entity relationship diagram and the detailed data content depicted in the data dictionary provide the basis for the data design activity. Part of data design may occur in conjunction with the design of software architecture. More detailed data design occurs as each software component is designed. The architectural design defines the relationship between major structural elements of the software, the design patterns that can be used to achieve the requirements the system architecture, the interface representation, and the component level detail.

The interface design describes how the software communicates within itself, with systems that interoperate with it, and with humans who use it. An interface implies a flow of information (e.g., data and/or control) and a specific type of behavior. Therefore, data and control flow diagrams provide much of the information required for interface design [19]. The component-level design transforms structural elements of the software architecture into a procedural description of software components. Information obtained from the PSPEC, CSPEC, and STD serve as the basis for component design.

IV. RESULTS AND DISCUSSIONS

A. TPA Working Process

TPA provides user request mode and auditing mode. User request mode gives the accessing permission from the cloud server. Auditing mode which establish the path to security auditing page. This is used to register the login to the web server. It contains name, password, address, and host name (online), security code. After registered authentication it will lead to the web server access into the cloud network.

This will auto generate after login to the web server. The users to gives permission to upload, download, reports the data from the user end. It will get through to the data upload/data download/reports directly. To upload the data into the web server, upload the data/files user have to encrypt the data and upload data command button. User can able to upload the data by both private and public segments.

In this process user gives the data path, and then encrypted the data by private and then uploaded the data into the web server. In this download the user have to specify the file name which was already uploaded into the database list and then user have to decrypt the data by using the authentication which was provided, and then only user have to download the data.

User report which is used to display the user name, file name, encrypt/decrypt file details, file mode. The auditing security gives data dynamics, data integrity, audit report results. Data dynamics provides the whole information about the time period which is data upload and downloaded details, but data integrity provides the private network details. In this case user selected the audit report option, and then it's waiting for audit request from server end to gather the information which was accessed.

B. Data Security in Cloud

The problem of data security in cloud data storage, which is essentially a distributed storage system. To ensure the correctness of users' data in cloud data storage need to propose an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append. Rely on erasure-correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability. By utilizing the homomorphic token with distributed verification of erasure coded data, the scheme achieves the integration of storage correctness insurance and data error localization, i.e., whenever data corruption has been detected during the storage correctness verification across the distributed servers, it shows guarantee the simultaneous identification of the misbehaving servers. Through detailed security and performance analysis, shows that the scheme is highly efficient and resilient to Byzantine failure, malicious data modification attack, and even server colluding attacks.

C. Threats to Security in the Cloud

Threats to security include:

A. Failures in Provider Security

Cloud providers control the hardware and the hyper visors on which data is stored and applications are run. Failures can threaten customers

B. Attacks by Other Customers

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

In the cloud, the entire infrastructure is shared among multiple customers. If proper isolation is not maintained, and the barriers between customers break down, one customer can potentially access another customer's data or interfere with another customer's applications. If one customer's environment is breached due to an outside attack, the effects of that attack must be contained within that customer's environment.

C. Availability and Reliability Issues

Cloud data centers like enterprise data centers are usually safe and secure. However, outages do occur. Also, the cloud is only usable through the Internet, so reliability and availability of the Internet and access to it are essential

D. Legal and Regulatory Issues

The virtual, international nature of cloud computing raises many legal and regulatory issues. Few of them are being sorted at the time this book is written

E. Perimeter Security Model Broken

Many organizations use a perimeter security model with strong security at the perimeter of the enterprise network. This model has been weakening over the years with outsourcing and a highly mobile workforce. Cloud computing strikes its death knell. The cloud is certainly outside the perimeter of enterprise control, but it will now store critical data and applications

F. Integrating Provider and Customer Security Systems

A unified directory and other components of security architecture such as automated provisioning, incident detection and response, are required. Does the cloud provider integrate with these or rely on manual provisioning and uncoordinated responses?

G. Unisys Secure Cloud Solution

Unisys Secure Cloud Solution is a managed cloud service providing com- prehensive data security for multi-tenant environments, in which clients share a common IT infrastructure. Because the solution uses Stealth technology, Unisys says enterprise clients can move existing business applications—including those with secure or sensitive data, such as human resources, financial, and healthcare information—into a managed, shared cloud service, without needing to rewrite or alter applications.

V. CONCLUSION

According to the problem of data security in cloud data storage, this is essentially to distributed storage system. To achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users, an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append is proposed. To reply on erasure-correcting code in the file distribution preparations to provide redundancy parity vectors and guarantees the data dependability. By utilizing the homo-morphic token with distributed verification of erasure-coded data, the scheme achieves the integration of storage correctness insurance and data error localization, i.e., whenever data corruption has been detected during the storage correctness verification across the distributed servers, to almost guarantee the simultaneous identification of the misbehaving servers. Considering the time, computation resources, and even the related online burden of users, to provide the extension of the proposed main scheme to support third-party auditing, where users can safely delegate the integrity checking tasks to third-party auditors and be worry-free to use the cloud storage services. Through detailed security and extensive experiment results, which show that the scheme is highly efficient and resilient to Byzantine failure, malicious data modification attack, and even server colluding attacks.

REFERENCES

[1] M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis, A. Vakali, "Cloud Computing Distributed Internet Computing for IT and Scientific Research," Vol.13, pp 10-15, Oct. 2009.

[2] L. Chang, L. Chin, A.Y. Chang, J. C .Chun, " Information security issue of enterprises adopting the application of cloud computing," IEEE 2010 Sixth International Conference on Networked Computing and Advanced Information Management (NCM), pp 645-649, Aug. 2010.

[3] R. Maggiani, "Cloud computing is changing how we communicate," 2009 IEEE International Professional Communication Conference, pp 1-6, Jul. 2009.

[4] L. Geng F. David Z. Jinzy D. Glenn, "Cloud computing: IT as Service, "IEEE computer society IT Professional," Vol. 11, pp.10-13, Apr. 2009.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

[5] Aman Bakshi, Yogesh B. Dujodwala, "Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine," ICCSN '10 Proceeding of the 2010 Second International Conference on Communication. Software and networks, pp. 260-264, 2010.

[6] B. R. Kandukuri, R. V. Paturi and A. Rakshit, "Cloud Security Issues," 2009 IEEE International Conference on Services Computing, pp. 517-520, Sep. 2009.

[7] K. Hwang, S Kulkarni and Y. Hu, "Cloud security with virtualized defense and Reputation-based Trust management," Proceedings of 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (security in cloud computing), pp. 621-628, Dec. 2009.

[8] Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage, "Hey, you get off my cloud: Exploring information leakage in third party compute clouds," CCS'09, Proceedings of the 16th ACM conference on Computer and Communications Security, pp. 199-212, 2009.

[9] L.J. Zhang and Qun Zhou, "CCOA: Cloud Computing Open Architecture," ICWS 2009: IEEE International Conference on Web Services, pp. 607-616. Jul. 2009.

[10] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, "Intrusion detection techniques for Grid and Cloud Computing Environment," IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43, 2010.

[11] Claudio Mazzariello, Roberto Bifulco and Roberto Canonico, "Integrating a Network IDS into an Open Source Cloud Computing Environment," Sixth International Conference on Information Assurance and Security, USA, pp. 265-270, Aug. 2010.

[12] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, "The Eucalyptus open-source cloud-computing system," in Proceedings of the 9th IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID '09), pp. 124–131, 2009.

[13] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing,"17th International workshop on Quality of Service, USA, pp.1-9, Jul. 2009.

[14] Marios D. Dikaiakos, Dimitrios Katsaros, Pankaj Mehra, George Pallis, Athena Vakali, "Cloud Computing: Distributed Internet Computing for IT and Scientific Research," IEEE Internet Computing Journal, vol. 13, issue.5, pp. 10-13, Sep.2009.

[15] R. Maggiani, Communication Consultant, Solari Communication, "Cloud Computing is Changing How we Communicate," 2009 IEEE International Professional Conference, IPCC, pp. 1-4, Waikiki, HI, USA, Jul. 2009.

[16] S. Pearson, "Taking account of privacy when designing cloud computing services," CLOUD '09 Proc. of ICSE Workshop on Software Engineering Challenges of Cloud Computing, pp. 44-52, IEEE Computer Society Washington, May 2009.

[17] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience," 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008.

[18] Lori M. Kaufman, "Data security in the world of cloud computing," IEEE Security and Privacy Journal, vol. 7, issue. 4, pp. 61-64, July- Aug 2009.

[19] Neal Leavitt, "Is Cloud Computing Really Ready for Prime Time" Computer, vol. 42, issue. 1, pp. 15-20, IEEE Computer Society, Jan. 2009.

AUTHOR BIOGRAPHY

D. Kanchana received the M.C.A. degree from Bharathidasan university in 2002. Currently, She is a Assistant Professor in the Department of Computer Applications, SRM University, Ramapuram campus, Chennai. Her research interests include Cloud Computing, network security and mobile computing.

Dr. S. Dhandapani received the B.E. degree in Electrical and Electronics Engineering and M.E. degree in Applied Electronics from Bharathiar university in 1998 and 2003 respecively and Ph.D. degree in Information and Communication Engineering from Anna university, Chennai in 2012. Currently, he is a Professor in Alpha College of Engineering, Chennai. He is a life member of ISTE. He has pubished more than 10 research papers. His research interests include digital image processing, network security and VLSI design.