Online Data Security for Secure Cloud Storage

N. Indira, M.Hemalatha, A.V. Kalpana, D. Rukmani Devi, S.Venkatesan

Abstract**:** ***The capacity benefit given by cloud server is not completely trusted by clients. In existing system, data can be modified and corrupted by the unauthorized user with the assistance of the employees. Typically the information are safely taken care of by the organization yet a few employees offered the specifiers to programmers for cash. Because of this issue, the information are not protected. Hence the advanced safe technology is used. The information are uploaded by the encryption design with video mode and the information are downloaded by the client with the assistance of face detection video mode, at that point the administrator acknowledge the solicitation by the face recognition video mode and information are shared starting from one place to another. Utilizing the AES algorithm the information is shared safely. It is implemented in both hardware and software. It utilizes higher length key sizes, for instance, 128, 192 and 256 bits for encryption. It is most basic security convention utilized for wide range of uses, for example, wireless communication, money related exchanges, e-business, encoded information storage and so forth.***

Keywords **:** ***Face Detection, Downloading file, Encryption, Uploading File, Video Mode.***

I. INTRODUCTION

Storing in a Cloud developing model of capacity to give adaptable, versatile and pay-as-you-use service to Cloud clients. For individual use, the endorsers appreciate the opportunity to access to their information anyplace, whenever with any gadget. At the point when cloud storage is used by a group of clients, it permits colleagues to synchronize and deal with every single shared documents. In addition, it likewise spares the client a lot of capital venture of costly expensive storage equipment. Cloud delivers convenience to the customers and simultaneously arouses many security and privacy problems. Since the information are physically put away on the numerous servers of the cloud service provider, the clients can't completely responsible for their information.

They stress over the protection of the stored documents since the server might be intruded by the hacker or the information could be abused by the internal staff for commercial reason. The customers like to receive the encryption technology to secure the information secrecy, which in the interim stimulates another issue: how to execute information recovery on the large volume of cipher text.

It is practically unbelievable to request that the cloud endorser download the majority of their stored data and after that decrypt and search on the recuperated plaintext reports. No client could endure the huge transmission overhead and the hanging tight time for the information recovery result. Accessible encryption innovation applies encryption assurance of the information, yet in addition supports proficient inquiry work without undermining the information protection. The information client produces a token of the substance that he needs to look through utilizing his private key. In the wake of getting the token, the cloud server looks on the encrypted data without decrypting the cipher text. The most noteworthy point is that the server adjusts nothing about the plaintext of neither the encrypted data nor the searching during the data recovery strategy.

Be that as it may, a large portion of the accessible encryption plots just help some fundamental search patterns, for example, single keyword search, conjunctive keyword search and Boolean search. Even though the cloud computing is a furious challenge to the industry, indispensable significance to give great client experience.

In a current framework, information are undermined by the unauthenticated client with the assistance of the employees. Typically the information are safely taken care of by the organization yet a few employees offered their entrance specifiers to the programmers for cash. Cloud computing is that the utilization of computing assets both hardware and software are serviced through a system.

Today, cloud computing generates lots of hype; it's each promising and scary. Businesses see its potential however even have several issues. Security is considered one among the foremost essential aspects in everyday computing, and it's no completely different for cloud computing because of the sensitivity and importance of information kept within the cloud. Cloud computing frameworks utilize new innovations and administrations, most that haven't been completely assessed as for security. Cloud Computing has many major problems and issues, like data security, trust, expectations, rules, and performance problems.

DRAWBACKS IN EXISTING SYSTEM

- The client can just sign documents on that specific PC.
- The private key security dependent completely on PC security.

Revised Manuscript Received on November 27, 2019.

***** Correspondence Author

N. Indira, Assistant Professor, Department of Computer Science and Engineering at Panimalar Engineering College, Chennai, Tamilnadu, India. indiranatarajan13@gmail.com

M. Hemalatha, Assistant Professor , Department of Computer Science and Engineering at Aalim Muhammed Salegh College of Engineering, Avadi, Chennai, Tamilnadu, India. hemalelangovan@gmail.com

A.V. Kalpana, Assistant Professor, Department of R. M. K Engineering College, Chennai, Tamilnadu, India. kalpanavijay21@gmail.com

Dr. D. Rukmani Devi, Professor Department of R.M.D Engineering College, Email: rdrukmani319@gmail.com

S.Venkatesan, Senior Manager, Tejas Networks Pvt. Ltd. Bangalore, India. Email: Venbose_271@yahoo.co.in

- Confidentiality is one amongst the most important problems round faced by cloud systems since the knowledge is keep at a remote location.
- Integrity is preventing the improper modification of data. Conserving integrity like confidentiality is another major issue round faced by cloud systems.

EXISTING SYSTEM

Confidentiality is one amongst the most important problems round faced by cloud systems since the knowledge is kept at a remote location. Integrity is preventing the improper modification of data. Conserving integrity like confidentiality is another major issue round faced by cloud systems.

II. RELATED WORK

1. The sender just has to know the beneficiary's identity, however no other data, (for example, their public key or declaration). The receiver must have its secret key put away on the PC and a one of a kind individual security gadget interfacing with the PC. All the more critically, when the security device is taken or lost, this device is disavowed. It can't be utilized to decode any ciphertext. This should be possible with Cloud server, quickly execute a few methods changed current encrypted text. It is totally straightforward to the sender.

2. PCM has been generally utilized in image examination and knowledge revelation.

Further, they structured a conveyed HOPCM strategy dependent on Map Reduce for a lot of heterogeneous information. At last, it devise a privacy preserving HOPCM algorithm (PPHOPCM), ensures the private particulars on cloud using application of BGV encryption plan to HOPCM. Here the capacities to refresh enrollment lattice and bunching focuses are approximated as polynomial capacities to help the safe registering of the BGV scheme.

4. This paper clarified the review, basis and parts in the CCAF to ensure information security. CCAF is represented by the framework configuration dependent on the prerequisites and the usage shown by the CCAF multi-layered security. Since, Data Center has 10 petabytes of information, there is a gigantic errand to give constant security and isolate.

5. A large number of data, usually referring to big data, have been generated from Internet of Things. This paper, shows a twofold projection profound computation model (DPDCM) for huge information highlight realizing, which ventures contributed to two separate subspaces in the shrouded layers to learn cooperated highlights of huge information by supplanting the concealed layers of the traditional profound calculation model (DCM) with twofold projection layers. Besides, they devise a learning calculation to prepare the DPDCM.

6. Remote information trustworthiness checking is of vital significance in cloud storage. It can cause the customers to check whether their re-appropriated information is kept unblemished without downloading the entire information. In some application situations, the customers need to store their information on multi-cloud servers. In any case, the test is that the computational weight is unreasonably tremendous for the clients with asset obliged devices to figure the public validation labels of file blocks.

8. The redistributing of information into the cloud inalienably requires a mechanism to control the entrance ability of the clients and the cloud suppliers. This instrument requires productive cryptographic natives to accomplish fine grained access control of information, proof of capacity, and repudiation of the approval.Thus, they presented a secure cloud data storage architecture with the features of dynamic user construction, revocation of the authorization, and proof of storage.

III. PROPOSED SYSTEM

In our proposed scheme, the data are uploaded by the encryption format with video mode. The data are shared in Encryption algorithm so unauthorized user are not accepting the data.

One strategy to achieving reliable computing in cloud inf rastructures is to adapt current reliable computing alternativ es to the cloud computing paradigm or to use them, these solutions as building blocks in new cloud design models. The foremost distinguished approach to trustworthy cloud computing technology are specific below this approach delivers a scalable cloud computing platform that Has end to end safety clients and end to end privacy.

The proposed framework will build security into its services in accordance with security best practices and documents the way to use the safety options. It is necessary that we leverage these safety features and best practices to style a befittingly secure application environment. Guaranteeing the integrity of confidentiality a nd information accessibility.

The registration is made by the person/employee. After registration he/she has to login. On successful login he/she can upload file. The content of uploaded file will be encrypted it will be securable .That file will be shared to four administrators. The person/employee who is the beneficiary of hacking any file for commercial purpose, need any file then they have to be register and login they can send a request for file. That request is sent to four administrators. If those four administrators accepted then only they can get that file. If any employee tried to hack any file then the administrators can find that person face by using of web camera app. So it simple to identify the hacker by allowing the request under video mode.

video mode.

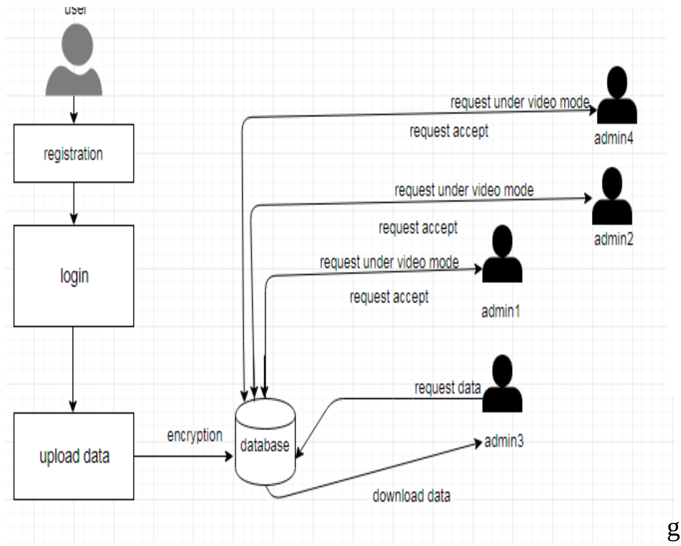


Fig.1. System Model

The important role for the user is to move login window to userwindow.

Users must enter the login I d and password in this login pa ge. It will check username and password is match or not (valid user id and valid password). If we enter some other incorrect username or password, a er ror message will be displayed. In this unauthorized user entering into the login window to user window can be prevented. It will provide a good security to store in database. So server contain user id and password and also check the authentication of the user. It well improves the security and preventing from unauthorized user entries into the network. In this module, validate the login user and server authentication for registration using JSP.

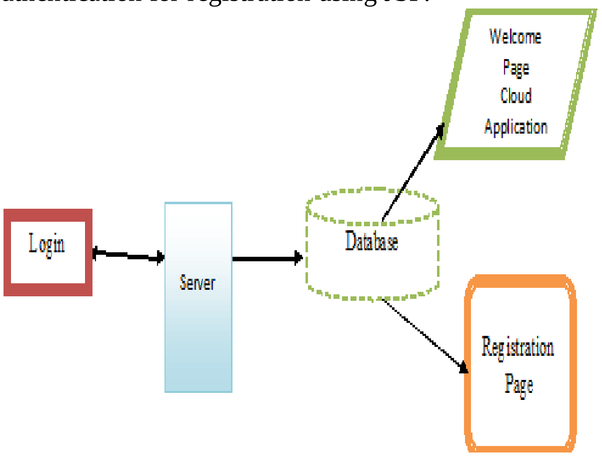


Fig.2. Design and implementation model

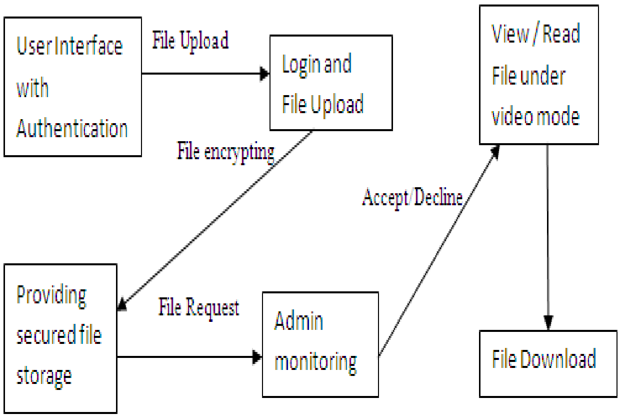


Fig.3. Proposed System Architecture

User id and password is verified and authenticated. After getting successful authentication the file is uploaded. User will login their account and upload a file, and that files are encrypted and stored in database. Even the file is uploaded, user cannot access the file before permission is granted by the admin to access.

It is not possible to obtain the uploaded file without the p roper administrator's consent. Administrators will monitor the files in the way of video mode. If anyone of the admin from the admin team wants to request a file, then the request will be passed by the video mode.

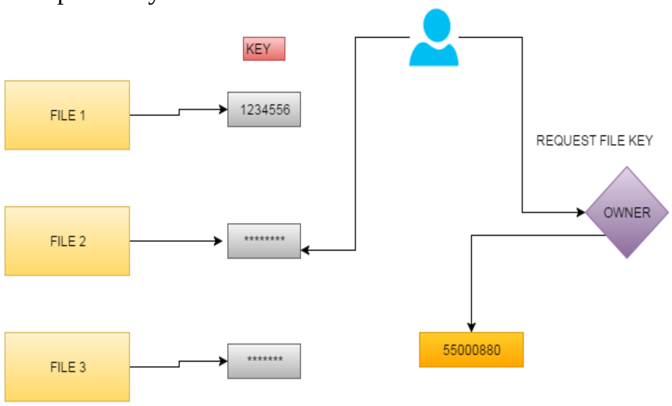


Fig.4. File access with keys

For reading each files which have been uploaded and spitted into 4 parts. The admin should be the owner of the file otherwise should know the four different key which have been combined by random algorithm. After reading the file admin can also download the file. If the file is accessed with wrong key then the content in the file cannot be downloaded.

IV. RESULT AND DISCUSSION

Our experiment is conducted on a system with PENTIUM IV 2.6 GHz, Intel Core 2 Duo. 4GB RAM 40 GB hard disk. Programs are built using JSP, Servlets and Java script. Back end for storing the user details using MY SQL 5.5. IDE used is Eclipse. AES is used for encrypting the file before storage. AES is an iterative as opposed to Feistel cipher. It depends on 'substitution–stage network'. It contains a progression of connected tasks, some of which

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

include supplanting contributions by explicit outputs (substitutions) and others include rearranging bits around (stages). Curiously, AES plays out the entirety of its calculations on bytes instead of bits. Thus, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are masterminded in four sections and four lines for preparing as a matrix. Unlike DES, the quantity of rounds in AES is variable and relies upon the length of the key.

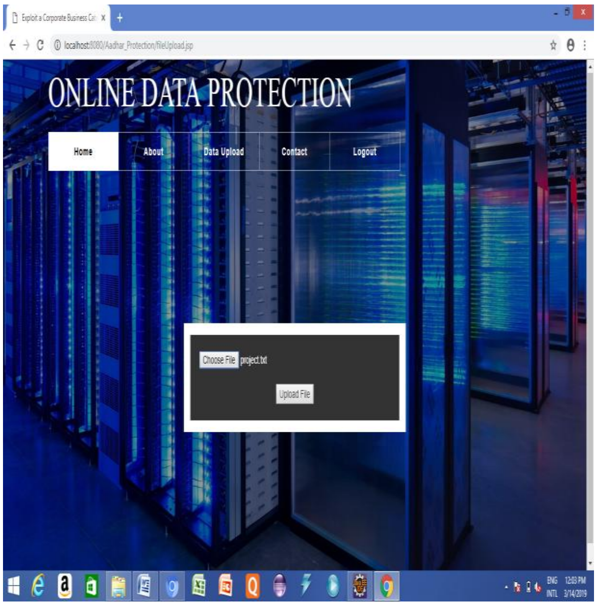
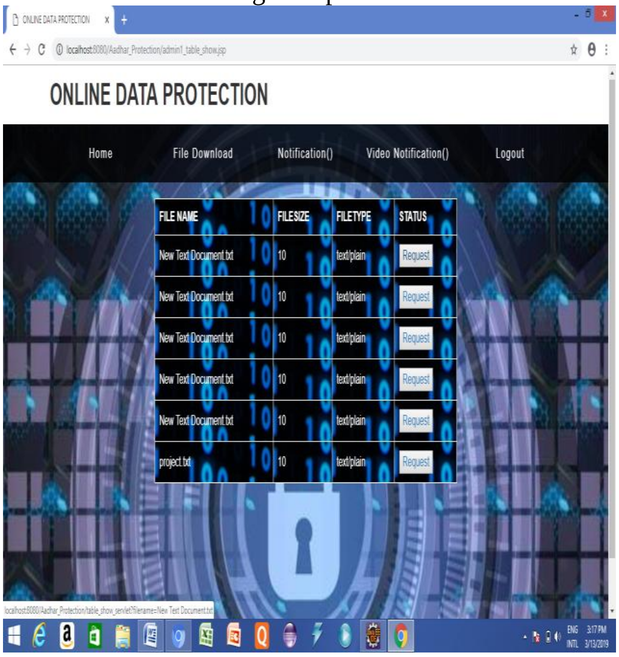
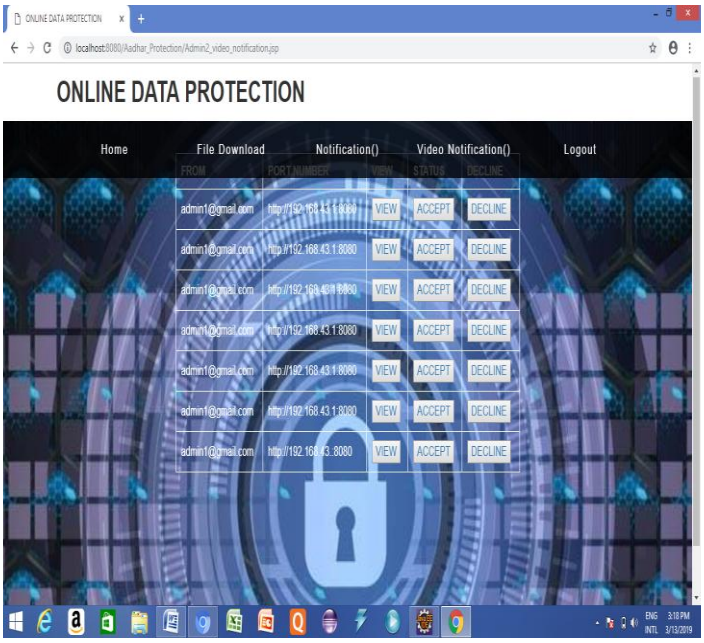


Fig. 5. Upload file


ONLINE DATA PROTECTION
localhost:8080/Aadhar_Protection/admin1_table_show.jsp
ONLINE DATA PROTECTION
Home
File Download
Notification()
Video Notification()
Logout
localhost:8080/Aadhar_Protection/table_show_servlet?filename=New Text Document.txt

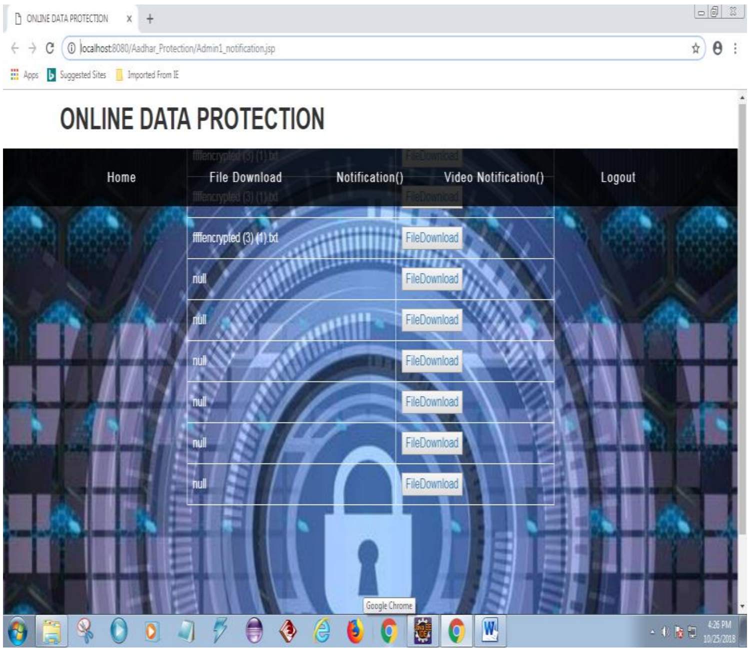
FILE NAME	FILESIZE	FILETYPE	STATUS
New Text Document.txt	10	text/plain	Request
New Text Document.txt	10	text/plain	Request
New Text Document.txt	10	text/plain	Request
New Text Document.txt	10	text/plain	Request
New Text Document.txt	10	text/plain	Request
project.txt	10	text/plain	Request

Fig. 6. File Request



FROM	PORT NUMBER	VIEW	STATUS	DECLINE
admin1@gmail.com	http://192.168.43.1:8080	VIEW	ACCEPT	DECLINE
admin1@gmail.com	http://192.168.43.1:8080	VIEW	ACCEPT	DECLINE
admin1@gmail.com	http://192.168.43.1:8080	VIEW	ACCEPT	DECLINE
admin1@gmail.com	http://192.168.43.1:8080	VIEW	ACCEPT	DECLINE
admin1@gmail.com	http://192.168.43.1:8080	VIEW	ACCEPT	DECLINE
admin1@gmail.com	http://192.168.43.1:8080	VIEW	ACCEPT	DECLINE
admin1@gmail.com	http://192.168.43.:8080	VIEW	ACCEPT	DECLINE

Fig.7. File Access



fffencrypted (3) (1).txt	FileDownload
null	FileDownload
null	FileDownload
null	FileDownload
null	FileDownload
null	FileDownload
null	FileDownload

Fig.8. File Download

V. CONCLUSION

A huge universe searchable authentication strategy to safeguard cloud storage system security, that performs frequent language encryption as well as DFA search functionality.The cloud service provider could test whether the encrypted regular language in the encrypted cipher text is acceptable by the DFA embedded in the submitted search token.No plaintext from either the regular language or the DFA will be disclosed to the cloud server in the test operation.Therefore the cloud service put forth a concrete construction with lightweight encryption and token generation algorithms. An example is given to show how the system works. The proposed scheme is privacy-preserving and indistinguishable against KGA, which are proved in standard model. The comparison and experiment result confirm the low transmission and computation overhead of the scheme.

VI. FUTURE ENHANCEMENTS

An accumulation is often needed to gather the partial results from these parallel executions in different servers. The runtime system captures new events and run corresponding actions to analyze the page and store more URLs into the URL set to generate new events. Visual cryptography (VC) is a method of encrypting a secret image into shares such that stacking a sufficient number of shares reveals the secret image. Shares are usually presented in transparencies.

REFERENCES

1. Liu J K, Liang K, Susilo W, et al. Two-factor data security protection mechanism for cloud storage system[J]. IEEE Transactions on Computers, 2016, 65(6): 1992-2004.
2. Zhang Q, Yang L T, Chen Z, Li P. PPHOPCM: Privacy-preserving High-order Possibilistic c-Means Algorithm for Big Data Clustering with Cloud Computing[J]. IEEE Transactions on Big Data, 2017, DOI: 10.1109/TBDATA.2017.2701816.
3. Q. Zheng, S. Xu, and G. Ateniese. VABKS: verifiable attribute-based keyword search over outsourced encrypted data. In INFOCOM, pp. 522C530. IEEE, 2014.
4. Chang V, Ramachandran M. Towards achieving data security with the cloud computing adoption framework [J]. IEEE Transactions on Services Computing, 2016, 9(1): 138-151.
5. Zhang Q, Yang L T, Chen Z, Li P. Privacy-preserving doubleprojection deep computation model with crowdsourcing on cloud for big data feature learning[J]. IEEE Internet of Things Journal, 2017, DOI: 10.1109/JIOT.2017.2732735.
6. Wang H. Identity-based distributed provable data possession in multicloud storage[J]. IEEE Transactions on Services Computing, 2015, 8(2): 328-340.
7. J, Tan X, Chen X, et al. Opor: Enabling proof of retrievability in cloud computing with resource-constrained devices[J]. IEEE Transactions on cloud computing, 2015, 3(2): 195-205.
8. Tiwari D, Gangadharan G R. A novel secure cloud storage architecture combining proof of retrievability and revocation[C]//Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on. IEEE, 2015: 438-445
9. Lucas SM, Reynolds TJ. Learning deterministic finite automata with a smart state labeling evolutionary algorithm. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2005 Jul;27(7):1063-74.
10. ViliamMalcher.Cloud computing design patterns[M]. Prentice Hall Press, 2016.
11. Zheng X H, Chen N, Chen Z, et al. Mobile cloud based framework for remote-resident multimedia discovery and access[J]. Journal of Internet Technology, 2014, 15(6): 1043-1050.
12. Chang V, Kuo Y H, Ramachandran M. Cloud computing adoption framework: A security framework for business clouds [J]. Future Generation Computer Systems, 2016, 57: 24-41.
13. Li Z, Dai Y, Chen G, et al. Toward network-level efficiency for cloud storage services[M]//Content Distribution for Mobile Internet: A Cloud-based Approach. Springer Singapore, 2016: 167-196.
14. Barsoum A. Provable data possession in single cloud server: A survey, classification and comparative study[J]. International Journal of Computer Applications, 2015, 123(9).

AUTHORS PROFILE

N. Indira is currently working in the Department of Computer Science and Engineering at Panimalar Engineering College, Chennai, Tamilnadu, India. She received her B.E degree in Computer Science and Engineering from Bharathidasan University, Thiruchirapalli, Tamilnadu, India and M.E degree in Computer Science and Engineering from Anna University, Chennai, Tamilnadu, India. She is now working toward the Ph.D degree at Anna University. Her research interests are Cloud Computing, Security systems and Computer Networks.

Mrs . M. Hemalatha, is currently working in the Department of Computer Science and Engineering at Aalim Muhammed Salegh College of Engineering, Avadi, Chennai, Tamilnadu, India. She received her B.E degree in Computer Science and Engineering from Bharathidasan University, Thiruchirapalli, Tamilnadu, India and M.E degree in Computer Science and Engineering from Anna University, Chennai, Tamilnadu, India. She has published papers in seven international journals, is now working towards the Ph.D degree at Anna University. Her research interests are Computer Networks, Cloud Computing, and Security systems. She is a Life member of ISTE.

A.V. Kalpana is currently an Assistant Professor in Computer Science and Engineering Department R. M. K Engineering College, Chennai, Tamilnadu, India. She obtained her B.E. from University of Madras, Chennai, Tamilnadu, India. She obtained her M. E. from Anna University, Chennai, Tamilnadu, India. Her research interests include Wireless Networks, Mobile Computing and Wireless Sensor Networks.

Dr. D. Rukmani Devi, is Professor in the Department of Computer Science and Engineering at R.M.D Engineering College where she has been a faculty member since June 2014. She obtained B.E in Electronics and Communication Engineering in the year 1992 from IRTT, affiliated to Bharthiyar University, M.S in Electronics in the year 1997 at BITS, Pilani and M.E. in VLSI Design in the year 2006 at R. M. K. Engineering College affiliated to Anna University. She has also completed Ph.D under Anna University in the area of VLSI Design. She has 22 years of teaching experience to UG classes and PG classes. She has guided many B.E. and M.E projects. She is guiding 13 Ph.D research scholars in her area. Her areas of interest include VLSI, Embedded, image and video processing and networks. She has published papers in seven international journals. She has delivered many lectures as resource person for many workshops, seminars and faculty development program sponsored by AICTE and Anna University. She has published book on 'VLSI Design' for the benefit of VI semester ECE students. She is a member of many professional societies like ISTE, SCIEI, CSTA, UACEE, ACM and IACSIT.