International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Secure and Multi Copy Dynamic Information Possession in Cloud System

Soumya N. S , Divya K. S, Deva Kumari A, Soumya. K, Sreeparna Chakrabarti

Abstract- Smart cities are implementation of information and communication technologies. These are developing based on institutional, physical, social and economic infrastructure. Every data is organized in a secure manner in these planned cities. Client's data is stored in Cloud servers Cloud Computing is that the net based mostly model, that permits the convenient on demand resources. More organisations are surging towards the cloud for outsourcing their sensitive data. Cloud Service Provider (CSP) can charge the client data based on their storage in the cloud server by paying fee, metered in Gigabytes/Month. For the scalability, availability and accessibility purpose, some customers want their data to be replicated in the multiple servers at the distinctive Data centers. If the customers want to store more copies of data in server, they have to pay more charges so it needs strong guarantee on CSP, that it stores all the data copies on the service contract agreement. This paper centers on a Data security of immense associations. A Mapping Based Dynamic Data possession scheme is proposed, to provide the guarantee to the customer that CSP isn't conning by putting away just barely any duplicates of information. This plan underpins Dynamic activities on the re-appropriated data.

Key Words- Dynamic Data, Cloud Computing, Data Migration, Intrusion Detection, Outsourcing data, Data Integrity

I. INTRODUCTION

Cloud Computing is the Utility based computing, which allows the user to access the resources pay as per the usage. Utility computing utilizes the cloud infrastructure for providing the business model to compute the services [1]. Recently more organisations are opting the cloud to store the huge amount of data. This data desires to keep secured in the cloud server. It promises the cost benefits, security and availability for business data. Cloud computing provides the Storage-as-a-service model to store the tremendous data by clients. Re-appropriating of the information to the remote Cloud Service Provider (CSP) licenses the customers to store a bigger number of information on the CSP than on the private Computer framework..

Manuscript published on January 30, 2020.
* Correspondence Author
Soumya N.S, A.P*, Department of Computer science and Engineering, MSEC, Bangalore, Ph: H: 9206488709, E-mail:soumya.yadav@gmail.com
Divya K.S, A.P, Department of Computer science, Kristujayanti College, Bangalore PH: 8884644346 E-mail: divyaks@kristujayanti.com
Deva Kumari A, A .P, Department of Computer Science, Kristujayanti College, Bengaluru, PH: 9600959444, E-mail: devakumari@kristujayanti.com
Soumya.K, A .P, Department of Computer science, Kristujayanti College, Bangalore, PH: 9645306611, Email: soumya.k@kristujayanti.com
Sreeparna Chakrabarti, A.P, Department of Computer science, Kristujayanti College, Bangalore, PH:8197832317 E-mail: sreeparna.c @kristujayanti.com

Such outsourced data storage endows the organisation or client to concentrate on the consistent server updates and other figuring issues. When the information has redistributed to the remote CSP, which may not be reliable. Information proprietor lacks the immediate authority over their delicate information

This absence of control raises the new testing assignments identified with the information security, classification and trustworthiness affirmation in the cloud computing.

Various techniques are available to support the data owner, to store their data to the untrusted cloud by providing confirmation identified with the confidentiality, integrity and access control. This idea is used to identify malicious activities from the CSP. The confidentiality issues can be resolved by encrypting the confidential data before outsourcing to the remote cloud servers. It gives the assurance for the owner's data. Data integrity refers to the validation of the data. PDP (Provable Data Possession) scheme is the one technique to authenticate the data integrity over the remote cloud [2]. Many researchers are focusing on problem of data outsourcing using various PDP methods.

PDP is a strategy for accepting information validation over remote server, where data holder sends copies of encrypted file to the remote Cloud Service Provider. Meanwhile small data structure called Meta data is stored in the Third Party Auditor (TPA) for the further verification purpose through Challenge Response protocol with the CSP [3]. Data owner outsources file to the CSP, which may be untrusted and erases the local copy of the file. To avoid this problem dynamic behaviour of data scheme is provided. In which the file is divided into multiple blocks and separate Mac Address will be generated to each block using the Hash function and MD5 Algorithms [4].

The proposed Mapping based Dynamic Data possession scheme directly deals with the multiple copies of the dynamic data. It allows the Data owner to modify the outsourced data as insertion, append and deletion of the existing data. The data efficiency refers to the Secure and Managed manner. The system integrity check fails when proving the multiple data copies. To deal with this issue corrupted copies are identified and slight modification can be done for the proposed scheme. This scheme allows the data migration between the Cloud Servers.

II. RELATED WORK

The Related work terms the background work done on various techniques and concepts related to the paper. The purpose of related work is to select the documents related to the project.

This provides the new ideas, information, data and evidence to fulfil the certain aims or views of the nature of the topic.

A. Efficient Remote Data Possession Infrastructures to Ensuring Data Storage.

The author Nalini et al. [5] proposed the remote data possession scheme. This scheme can be validated through Third Party Auditor (TPA) by verifying the uncorrupted copies. In this work the author used the Seb'e et al's protocol to support the efficient data possession of the critical information without the help of TPA. This design allows the auditor to communicate with the cloud by low communication costs. In addition to this work the audit results ensure the data correctness storage guarantee and the data error localization i.e., misbehaving remote server is identified. A security review of the proposed protocol indicates the protection of t he untrusted client and the TPA Verifier. The Seb'e et al's protocol has the following polynomial algorithms: Setup, TagGen, Challenge, Gen-proof and Check proof. It supports the dynamic environment.

B. Provable data possession scheme and uncheatable data transfer.

The author Decio Luiz et al. [6] [7] determines the specific RSA based secure Hash function is a Homomorphic. In this, work the author describes the protocol that prevents the cheating in data transfer. The outsourced data can secure through the Third Party Auditor. The verifier is not required to have the data related to the auditing, yet rather small Hash Function of the data is required. This convention is provable secure than the number factoring. Public key was used in this model as the RSA modulus. It is one of the advantages than the huge key generation for large data. This protocol is versatile and it does not fix the message size for given parameters or data. This protocol is useful in the distributive data stored in the multiple systems.

III. PROBLEM STATEMENT

Cloud Computing deals with the dynamic data. Outsourcing of a file should provide the scalability for dynamic data. Before outsourcing to the cloud data file is encrypted and divide into multiple blocks. If any modifications are required for the portion of the file, that portion has to be decrypted. The CSP should provide the guarantee for clients data based on service contract. Data files should be migrated between cloud servers. Mutual trust is established between the Data owner and CSP.

IV. PROPOSED METHODOLOGY

The proposed Methodology describes the Existing system and the features of proposed system.

A. Existing System

The Data owner or an Organisation can store their sensitive data to the CSP, which may not be trustworthy. Once the data is outsourced, data owner lacks the direct monitoring over their data. This lack of control creates the new issues like Confidentiality and Integrity. Only Single copy of Static data is outsourced. Only the Authorised users or a set of owner's clients can access this.

Disadvantages of Existing System:

There is no trust on the CSP that it utilising the allocated space for the Owner on the service contract. Utilization of the allocated space is neither effective nor efficient.

B. Proposed System

In Proposed system, Mapping Based Provable Multicopy Dynamic Data Possession is used. In this scheme, the outsourced file has to encrypt and divided into multiple data blocks. These blocks are stored on the CSP [1]. The owner can modify the outsourced data using Block operations like insertion, deletion, update and delete the existing copies of the files. Once the data has been outsourced, a Metadata small data structure is generated and stores in Block Status Table (BST). BST is stored on TPA for the further verification purpose. BST uses the data size has 8 bytes (two integers). Separate MAC Address will be generating for each block using the Secure Hash Algorithm (SHA-1) and Message Digest (MD5) [8].

Data Encryption and Decryption can be done using the AES Public key generation algorithm. Using RSA standard, Public Key and Private Keys are generated. When the authorised user wants to access the files stored on cloud server, he requires the shared Secret Key from the cloud and decrypt key from the owner. Challenge response protocol is used to verify the data in cloud. There will be a direct communication between the Data owner and the CSP [9]. The proposed system can be implementing in the Rack space public Cloud

Advantages of Proposed System

- This proposed scheme deals with the multiple copies of dynamic data.
- This provides a proof for Owner's data in the cloud.
- It provides the direct contact between the Data owner and the End User. This model may use in the any practical Applications like e-Health organisations.

IV. SYSTEM MODEL IMPLEMENTATION

In Cloud Computing System, it offers the storage-as-a-service model to store the user's data. The figure 1.1 shows the Architecture of the Cloud System Model. The implemented model consists of Cloud Service Provider, Cloud Servers, Data owner, User and Third Party Auditor module. The Data owner or an organisation can send the data to the CSP. Before sending, the data file is encrypted and divides into five blocks then stores the data to CSP. It chooses the different cloud servers to store the data due Security and Accessibility purpose. CSP is having all the local copy of owner files and migrated files along with their Secret key. The individual Cloud Server can store the files separately along with the contents. If any attacker tries to modify the contents of the files stored in the Cloud server, it blocks the Particular Attacker. Cloud Server allows the owner to modify the contents. To refresh the data of cloud server, data refreshes is scheduled, so it automatically refreshes the data. The Data owner can migrate the files from one server to another server. If any attacker or not registered user from outside can tries to modify the file contents of the file.

CSP automatically blocks the IP address of that intruder. In the owner module, modify the contents of the stored file in CSP, so it creates the direct connection between the owner and the CSP.

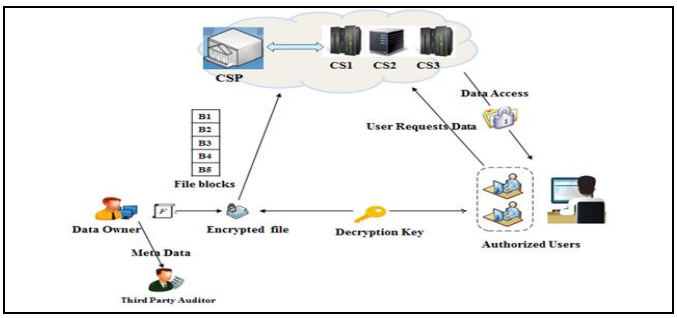


Fig. 1.1 Cloud System Model

During uploading data, it creates the small data structure called Meta data stored in the third-Party Auditor. This Meta data is stored in the Block Status Table of TPA, which contains the Mac address and Hash functions of the particular files but not the full contents. The contents are not stored in the TPA due to the security concerns. TPA also stores the all Owner's and user details. TPA checks the Data Integrity of the file by comparing the
MAC address stored in it with the file Mac Address stored in the Cloud Service Provider.

The authorised receiver or owner clients can access the file form the server. User requests the cloud to access the files, Cloud merge the file blocks and sends the decrypted

file to user. After receiving the file from Cloud server, user requests the decrypt key from the Data owner to decrypt the file. The data owner sends the key, using that key user can receive the file contents.

The connection between the client and server is takes place through the Networking Remote Method Invocation (RMI) method. Socket interface is created for every connection between the client and server. To implement this scenario Rack space cloud is used. Rack space a virtual cloud severs are used to implements the real scenario [10]. Open Stack Community powers it. It support the public, private and hybrid cloud infrastructures. To access the services of this cloud REST ful API is used, in which cloud files are mounted in local drive of the supported operating system like Linux, Ubuntu, Windows and Mac OS.

VI .ALGORITHM FOR CHALLENGE RESPONSE PROTOCOL.

In Challenge-Response protocol, owner or verifier (TPA) can challenge to the CSP to check the file integrity. Remote Server responding that all file copies are stored. Verifier or TPA compares the MAC address of the file stored in sever with local copy of owner file.

Table I: Challenge-Response Protocol

Input: Sk,Pk, Client Metadata D
Output: Proof for Data Integrity

Setup:
- Generate RSA modules n=ab (a & b are two prime numbers)
- Public key, Pk={e,n} and Secret key, Sk={d,n}
- Pseudo random function, p
- File of m blocks, F={b1, b2, b3,……,bm}
- Pseudo random generator, g
- Owner generates the Tag set Tj for each block.

Where Tj=g bj mod n & Tj={Sk, F'}
Challenge-Response:
Verifier/ Data owner (Challenge)
Remote server (Response)
Step 1: Generates the random key r
Step 2: Compute the no. of blocks to be challenge, chal
Step 3: Compute gs=gs mod n,(s € RZn)

Step 4:
Proof, P←Prove (F', Tj, chal)
Step 5:
Verify, V←ve .C, D

Step 6: Compare V and P, return 1 for successful verification.

VII. RESULT ANALYSIS

This section explains the performance the proposed system with outcomes.

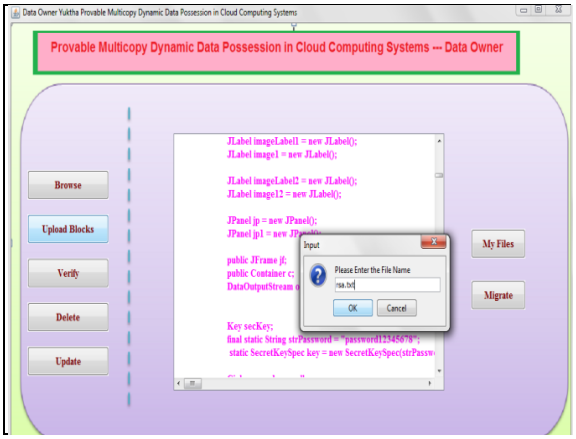
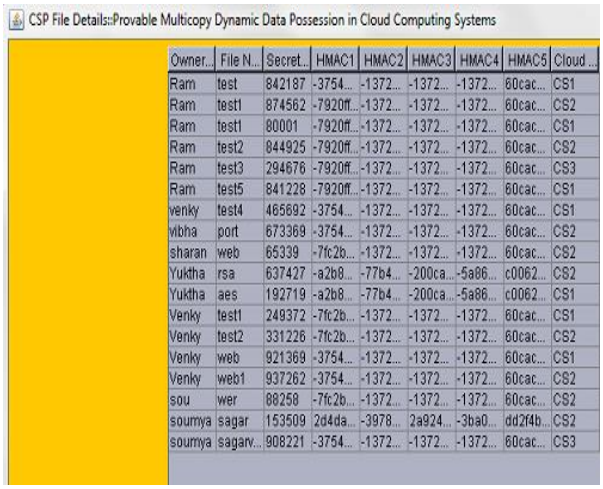


Fig. 1.2 Uploading file to the Cloud.

Figure 1.2 shows that Owner can browse the file and uploaded to Cloud Server. This file will be encrypts and divides into five blocks.



Owner...	File N...	Secret...	HMAC1	HMAC2	HMAC3	HMAC4	HMAC5	Cloud...
Ram	test	842187	-3754...	-1372...	-1372...	-1372...	60cac...	CS1
Ram	test1	874562	-7920ff...	-1372...	-1372...	-1372...	60cac...	CS2
Ram	test1	80001	-7920ff...	-1372...	-1372...	-1372...	60cac...	CS1
Ram	test2	844925	-7920ff...	-1372...	-1372...	-1372...	60cac...	CS2
Ram	test3	294676	-7920ff...	-1372...	-1372...	-1372...	60cac...	CS3
Ram	test5	841228	-7920ff...	-1372...	-1372...	-1372...	60cac...	CS1
venky	test4	465692	-3754...	-1372...	-1372...	-1372...	60cac...	CS1
vibha	port	673369	-3754...	-1372...	-1372...	-1372...	60cac...	CS2
sharan	web	65339	-7fc2b...	-1372...	-1372...	-1372...	60cac...	CS2
Yuktha	rsa	637427	-a2b8...	-77b4...	-200ca...	-5a86...	c0062...	CS2
Yuktha	aes	192719	-a2b8...	-77b4...	-200ca...	-5a86...	c0062...	CS1
Venky	test1	249372	-7fc2b...	-1372...	-1372...	-1372...	60cac...	CS1
Venky	test2	331226	-7fc2b...	-1372...	-1372...	-1372...	60cac...	CS2
Venky	web	921369	-3754...	-1372...	-1372...	-1372...	60cac...	CS1
Venky	web1	937262	-3754...	-1372...	-1372...	-1372...	60cac...	CS2
sou	wer	88258	-7fc2b...	-1372...	-1372...	-1372...	60cac...	CS2
soumya	sagar	153509	2d4da...	-3978...	2a924...	-3ba0...	dd2f4b...	CS2
soumya	sagarv...	908221	-3754...	-1372...	-1372...	-1372...	60cac...	CS3

Fig. 1.3 Files stored in Cloud Service Provider.

Figure 1.3 shows that the owner files are stored by CSP along with the Secret key and Hash function.

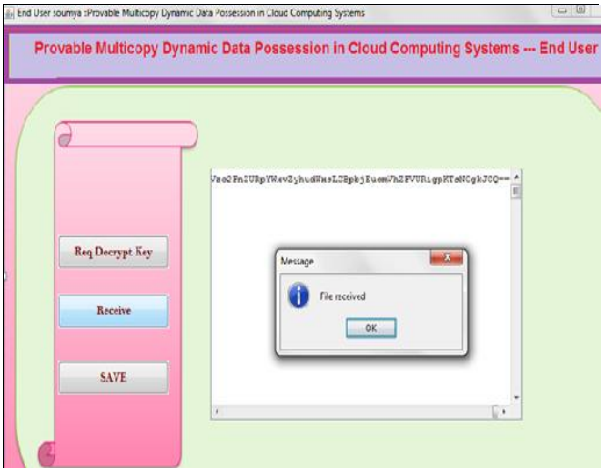


Fig. 1.4 Authorized user receiving file from Cloud Server

Figure 1.4 tells that the authorized user can login to the cloud and access the files. Cloud system ddecrypts the file using the key sent form the owner.

VIII. CONCLUSION

Remote cloud Server stores the data outsourced by the owner. It minimizes the burden of problems of problems with local data and maintenance issues. This paper concentrated on the problem of creating the multiple copies of file and checks the integrity against the untrusted cloud. In this work, new PDP scheme such as Mapping based technique is used. This scheme provisions the dynamic behavior of multi copy for a file. It allows the Data owner to update and scales the outsourced files. It provides the interaction between the CSP and Data owner by sharing the single secret key.

The proposed scheme focuses on arbitrary Auditing, Integrity, Verifiability and Efficiency of data. This scheme reduces the computation time and storage overhead compared to reference Tree Based Scheme. Reference model of PDP scheme uses the single copy of file. The corrupted data copies can be identified using the TPA auditing and reconstruct from the full damage with duplicate copies of file stored in another Cloud Server. So this scheme provides the more secure and efficiency for data. This paper focuses on a Data security of huge organizations like e-Health organizations, e-Government and Educational Institutions. In proposed scheme, it stores the important data in Cloud instead of storing in the local Client machines.

REFERENCES

1. Ayad F. Barsoum and M. Anwar Hasan "Provable Multicopy Dynamic Data Possession in Cloud Computing Systems" IEEE Transaction on information and security, Vol. 10, No. 3 March 2015.
2. P. Sathyabama Gayathri, J. Angela Jennifa sujana, T.Revathi " Enhancing security of Dynamic Data for storage services in cloud computing" IJIRSET International Conference Volume 3, Special Issue 3, March 2014.
3. Cong Wang, Qian Wang, Kui Ren1 and Wenjing Lou "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing" IEEE INFOCOM 2010, San Diego, CA, March 2010.
4. R.Bindu, U.Veeresh, Dr. S. Prem Kumar "Provable Multicopy Dynamic Data Possession in Cloud Computing Systems" International Journal of Computer Engineering In Research Trends Volume 3, Issue 1, January-2016, pp. 6-12.
5. Dr. T.Nalini, Dr.K.Manivannan,Vaishnavi Moorthy "Efficient Remote Data Possession Checking In Critical Information Infrastructures Ensuring Data Storage Security In Cloud Computing", IJIRCCE, Vol. 1, Issue 1, March 2013.
6. Cong Wang, Student Member, IEEE, Qian Wang, Kui Ren, Member, IEEE, Ning Cao, "Towards Secure and Dependable Storage Services in Cloud Computing" and Wenjing Lou, IEEE-2011.
7. D´ecio Luiz Gazzoni Filho, Paulo S´ergio Licciardi Messeder Barreto "Demonstrating data possession and uncheatable data transfer".
8. William Stallings, "Cryptography and Network Security: principles and practices" Sixth Edition, published by Pearson Education Inc. 2014.
9. Zhuo Hao, Sheng Zhong, and Nenghai Yu. "A privacy-preserving remote data integrity checking protocol with data dynamics and public veri_ability". IEEE Transactions on Knowledge and Data Engineering, 99(PrePrints), 2011.
10. Rackspace Cloud Infrastructure url: www.rackspace.com/en-in/cloud.
11. C. Wang, Q. Wang, K. Ren, and W. Lou.
12. (2009). "Ensuring data storage security in cloud computing," IACR Cryptology ePrint Archive, Tech.
13. Rep. 2009/081. [Online]. Available: http://eprint.iacr.org/
14. C. Erway, A. Küpçü, C. Papamanthou, and R.
15. Tamassia, "Dynamic provable data possession," in
16. *Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2009, pp. 213–222.
17. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou,
18. "Enabling public verifiability and data dynamics for storage security in cloud computing," in *Proc. 14th Eur. Symp. Res. Comput. Secur. (ESORICS)*, Berlin, Germany, 2009, pp. 355–370.
19. Z. Hao, S. Zhong, and N. Yu, "A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability," *IEEE Trans. Knowl. Data Eng.*, vol. 23, no. 9, pp. 1432–1437, Sep. 2011.
20. A. F. Barsoum and M. A. Hasan. (2010).
21. "Provable possession and replication of data over cloud servers," Centre Appl. Cryptograph. Res., Univ.
22. Waterloo, Waterloo, ON, USA, Tech. Rep. 2010/32.
23. [Online]. Available: http://www.cacr.math.uwaterloo.ca/techreports/2010/ cacr2010-32.pdf
24. Z. Hao and N. Yu, "A multiple-replica remote data possession checking protocol with public verifiability," in *Proc. 2nd Int. Symp. Data, Privacy, E-Commerce*, Sep. 2010, pp. 84–89.
25. H. Shacham and B. Waters, "Compact proofs of retrievability," in *Proc. 14th Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, 2008, pp. 90–107.
26. A. Juels and B. S. Kaliski, Jr., "Pors: Proofs of retrievability for large files," in *Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS)*, 2007, pp. 584-597
27. R. Curtmola, O. Khan, and R. Burns, "Robust remote data checking," in *Proc. 4th ACM Int. Workshop Storage Secur. Survivability*, 2008, pp. 63-68
28. K. D. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: Theory and implementation," in *Proc. ACM Workshop Cloud Comput. Secur. (CCSW)*, 2009, pp.

AUTHORS PROFILE

Ms. Soumya N.S is working as Assistant Professor in Computer Science Department in M.S. Engineering College, Bengaluru, India. She has completed her B.E in Computer Science and Engineering and MTech in Network Engineering. Soumya has published a handful papers in National and International journals in the area of computer network and cryptography. She has cleared UGC NET,December 2018 with good score. She is currently pursuing her Ph.D. in the area of Cryptography and Network security. She is enthusiastic in continuous learning and has completed certification programs

Ms. Divya K. S, is a research scholar, working as Assistant Professor in Computer Science Department in Kristu Jayanti College, Bengaluru, India. She has completed her Engineering in Computer Science and Engineering and M.Tech in Software Engineering. She is currently pursing Ph.D in the area of Network Security. Divya has published research papers in the area of cryptography, AI,IoTs,Computer networks , and Network security.She has 12 years of teaching experience in reputed Engineering colleges. She completed a funded project from Karnataka Government (KCST) in the year of 2018. She was the author of a text book in Operation Research

Ms. A.Deva Kumari, is currently working as Asst. Professor in Kristu Jayanti College (Autonomous), Bengaluru, Karnataka, India. She has completed her B.E in Computer Science from East Point College of Engineering and Technology and M.E in Computer Networks from University Visvesvaraya College of Engineering, Bengaluru. She is GATE 2010 qualified. She has 5 years of teaching experience including Engineering Colleges; she also has guided engineering student's projects in the area of computer networks and IoT. She has presented paper in international conference. Her area interest includes computer networks, cloud computing, Data mining and AI

Soumya K , working as a assistant professor of computer science department in Kristujayanti college(Autonmous), Bangalore. She has completed Bsc computer science and Masters in computer application. She has presented papers in national conference in the area of Data mining and Internet of things she has cleared UGC NET in December 2018 with good score.Her research interests include Data Mining, Cloud Computing.

Sreeparna Chakrabarti, is currently working as an Assistant Professor at Kristu Jayanti College (Autonomous) and perusing Ph.D from Visvesvaraya Technological University. She has over 8 years of experience in teaching field and guided more than 30 MCA final year students in their major project. She started her PhD in 2017 under VTU.Her research interests include Cryptography, Network Security, Cloud Computing, and Machine Learning. She is a lifetime member of ISTE and IENG.