IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 6.252

Volume 2, Issue 7, May 2022

Data Security and Privacy Protection for Cloud Storage

Chittumothu Srividhya[1] and Deepthi B[2]
Department of Information Technology
Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, Tamil Nadu

Abstract: *In this paper, we focus on the development of cloud computing technology with the explosive growth of unstructured data, cloud storage technology gets more attention and better development. The cloud provider does not have suggestions regarding the information and the cloud data stored and maintained globally anywhere in the cloud. The privacy protection schemes are usually based on encryption technology. There are many privacy preserving methods in the side to prevent data in cloud. We propose a three-layer storage framework based on fog computing. The proposed framework can both take full advantage of cloud storage and protect the privacy of data. Here we are using Hash-Solomon code algorithm is designed to divide data into different parts. If the one data part missing we lost the data information. In this framework we are using bucket concept based algorithms and secure the data information and then it can show the security and efficiency in our scheme. Moreover, based on computational intelligence, this algorithm can compute the distribution proportion stored in cloud, fog, and local machine, respectively Software as a Service (SaaS): Client releases their application on a hosting environment which can be accessed through network from various clients by application users. The client does not manage or control the underlying cloud infrastructure with the possible exception of limited user-specific application configuration settings. Google Apps and Microsoft Office 365 are the examples for SaaS..*

Keywords: Data security, privacy of data in each server, bucket concept, recovery of lost data

I. Introduction

Cloud storage also causes a series of secure problems. When using cloud storage, users do not actually control the physical storage of their data and it results in the separation of ownership and management of data. In order to solve the problem of privacy protection in cloud storage, we propose a TLS framework based on fog computing model and design a Hash-Solomon algorithm. Through the theoretical safety analysis, the scheme is proved to be feasible. By allocating the ratio of data blocks stored in different servers reasonably, we can ensure the privacy of data in each server. On another hand, cracking the encoding matrix is impossible theoretically. Besides, using hash transformation can protect the fragmentary information. Through the experiment test, this scheme can efficiently complete encoding and decoding without influence of the cloud storage efficiency. The three layer cloud storage stores in to the three different parts of data parts .If the one data part missing we lost the data information. By this method, the attacker cannot recover the user's original data even if he gets all the data from a certain server. As for the CSP, they also cannot get any useful information without the data stored in the fog server and local machine because both of the fog server and local machine are controlled by users.

II. LITERATURE SURVEY

A. Preserving Security Solution For Cloud Services

A novel privacy-preserving security solution for cloud services. Our solution is based on an efficient nonbilinear group signature scheme providing the anonymous access to cloud services and shared storage servers. The novel solution offers anonymous authentication for registered users. Thus, users' personal attributes (age, valid registration, successful payment) can be proven without revealing users' identity, and users can use cloud services without any threat of profiling their behaviour. However, if a user breaks provider's rules, his access right is revoked. Our solution provides anonymous access, unlinkability and the confidentiality of transmitted data. We implement our solution as a proof of concept application and present the experimental results. Further, we analyze current privacy preserving solutions for cloud services and group signature schemes as basic parts of privacy enhancing solutions in cloud services. We compare the performance of our solution with the related solutions and schemes.

DOI: 10.48175/IJARSCT-4447

B. Secure Data Privacy Preservation for On-Demand Cloud Service

A novel hand gesture recognition algorithm based on Kinect. Using the depth and skeleton from Kinect, mark-less hand extraction is achieved. The hand shapes (depth) and corresponded textures (color) are represented in the form of super pixels, which better retain the overall shapes and color of the gestures to be recognized. Based on this representation, a novel distance metric, Super pixel Earth Mover's Distance (SP-EMD), is proposed to measure the dissimilarity between the hand gestures. The effectiveness of the proposed distance metric and recognition algorithm is illustrated by experimental results and a high mean accuracy of 98.8% for hand gesture recognition is achieved based on the joint color-depth SP-EMD.

C. Survey On Secure Services In Cloud Computing

Cloud computing is an emerging technology and it is purely based on internet and its environment. It provides different services to users such as Software-as-a-Service (SaaS), PaaS, IaaS, Storage-as-a-service (SaaS). Using Storage-as-a-Service, users and organizations can store their data remotely which poses new security risks towards the correctness of data in cloud. In order to achieve secure cloud storage, there exists different techniques such as flexible distributed storage integrity auditing mechanism, distributed erasure-coded data, Merkle Hash Tree(MHT) construction etc. These techniques support secure and efficient dynamic data storage in the cloud. This paper also deals with architectures for security and privacy management in the cloud storage environment.

D. On A Relation Between Verifiable Secret Sharing Schemes And A Class Of Error- Correcting Codes

We try to shed a new insight on Verifiable Secret Sharing Schemes (VSS). We first define a new “metric” (with slightly different properties than the standard Hamming metric). Using this metric we define a very particular class of codes that we call error-set correcting codes, based on a set of forbidden distances which is a monotone decreasing set. Next we redefine the packing problem for the new settings and generalize the notion of error correcting capability of the error-set correcting codes accordingly (taking into account the new metric and the new packing). Then we consider burst-error interleaving codes proposing an efficient burst-error correcting technique, which is in fact the well-known VSS and Distributed Commitments (DC) pair-wise checking protocol and we prove the error-correcting capability of the error-set correcting interleaving codes.

F. A Secure Cloud-Assisted Urban Data Sharing Framework For Ubiquitous-Cities

With the accelerated process of urbanization, more and more people tend to live in cities. In order to deal with the big data that are generated by citizens and public city departments, new information and communication technologies are utilized to process the urban data, which makes it more easier to manage. Cloud computing is a novel computation technology. After cloud computing was commercialized, there have been lot of cloud-based applications. Since the cloud service is provided by the third party, the cloud is semi-trusted. Due to the features of cloud computing, there are many security issues in cloud computing. Attribute-based encryption (ABE) is a promising cryptography technique which can be used in the cloud to solve many security issues. In this paper, we propose a framework for urban data sharing by exploiting the attribute-based cryptography. In order to fit the real world ubiquitous-cities utilization, we extend our scheme to support dynamic operations. In particular, from the part of performance analysis, it can be concluded that our scheme is secure and can resist possible attacks. Moreover, experimental results and comparisons show that our scheme is more efficient in terms of computation..

III. EXISITING SYSTEM

Recent years witness the development of cloud computing technology. With the explosive growth of unstructured data, cloud storage technology gets more attention and better development. the computer technology has developed rapidly. Cloud computing has gradually matured through so many people effort’s. In current storage schema, the user’s data is totally stored in cloud servers. If the user lose their right of control on data and face privacy risk. The privacy protection schemes are usually based on encryption technology. These kinds of methods cannot effectively resist attack

from the inside of cloud server. Changes in the understanding of risk as a result of extending the datacentre into the cloud. Low latency and location awareness

IV. PROPOSED SYSTEM

The framework can take full of cloud storage and protect the privacy of data.Here the cloud computing has attracted great attention from different sector of society.The three layer cloud storage stores in to the three different parts of data parts .If the one data part missing we lost the data information. In this proposed framework using the bucket concept based algorithms.In our system we using a bucket concept so reduce the data wastages and reduce the process timings.

We are using a BCH (Bose–Chaudhuri–Hocquenghem) code algorithm. It's High flexible. BCH code are used in many communications application and low amount of redundancy.

V. SYSTEM ARCHITECHTURE

A Three-Layer Privacy Preserving Cloud Storage Scheme Based on Computational Intelligence in Fog Computing**.** The privacy preservation is our focus, some active attacks are beyond the scope of this work. The three layer cloud storage stores in to the three different parts of data parts .If the one data part missing we lost the data information. In this proposed framework using the bucket concept based algorithms. We are using a BCH code algorithm. It's High flexible.

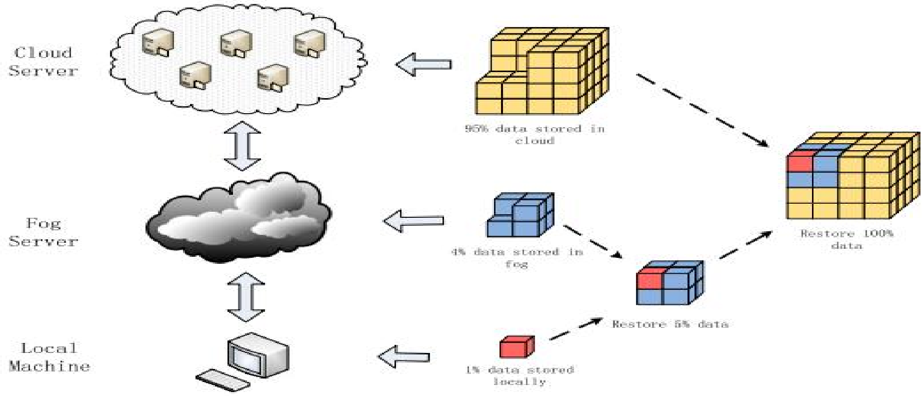


Fig-1: SYSTEM ARCHITECTURE

VI. ALGORITHM USED

A. BUCKET

The Bucket Access Controls resource represents the Access Control Lists (ACLs) for buckets within Google Cloud Storage. ACLs let you specify who has access to your data and to what extent.

The three layer cloud storage stores in to the three different parts of data parts .If the one data part missing we lost the data information. In this proposed framework using the bucket concept based algorithms.

B. BCH CODE ALGORITHM

The Bose, Chaudhuri, and Hocquenghem (BCH) codes form a large class of powerful random error-correcting cyclic codes. This class of codes is a remarkable generalization of the Hamming code for multiple-error correction.We only consider binary BCH codes in this lecture note. Non-binary BCH codes such as Reed-Solomon codes will be discussed in next lecture note.

VII. CONCLUSION

The development of cloud computing brings us a lot of benefits. Cloud storage is a convenient technology which helps users to expand their storage capacity. However, cloud storage also causes a series of secure problems. When using cloud storage, users do not actually control the physical storage of their data and it results in the separation of ownership and managementofdata.Inordertosolvetheproblemofprivacyprotectionincloud storage, we propose a TLS framework based on fog computing model and design a BCH Code algorithm. Through the theoretical safety analysis, the scheme is proved to be feasible. By allocating the ratio of data blocks stored in different servers reasonably, we can ensure the privacy of data in each server. On another hand, cracking the encoding matrix is impossible theoretically. Besides, using hash transformation can protect the fragmentary information. Through the experiment test, this scheme can efficiently complete encoding and decoding without influence of the cloud storage efficiency. Furthermore, we design a reasonable comprehensive efficiency index, in order to achieve the maximum efficiency, and we also find that the Cauchy matrix is more efficient in coding process.

DOI: 10.48175/IJARSCT-4447

VIII. FUTURE ENHANCEMENT

In future, we are going to implement real-time cloud in this concept like amazon web services for additional security.

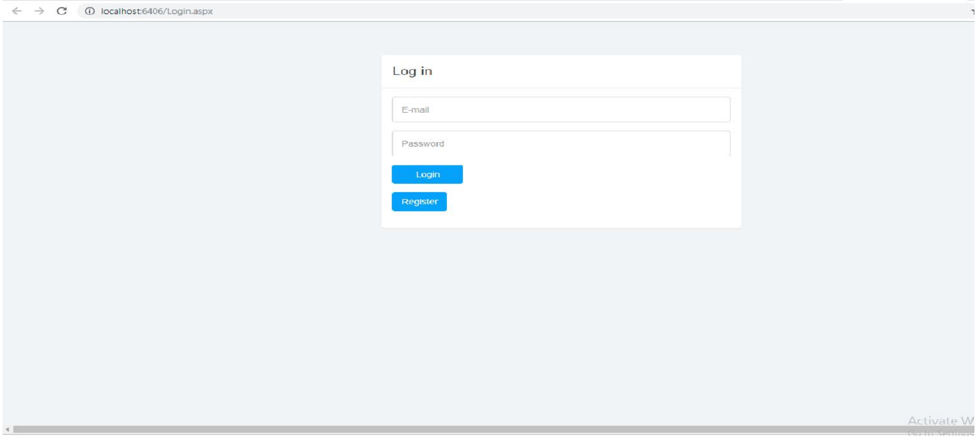
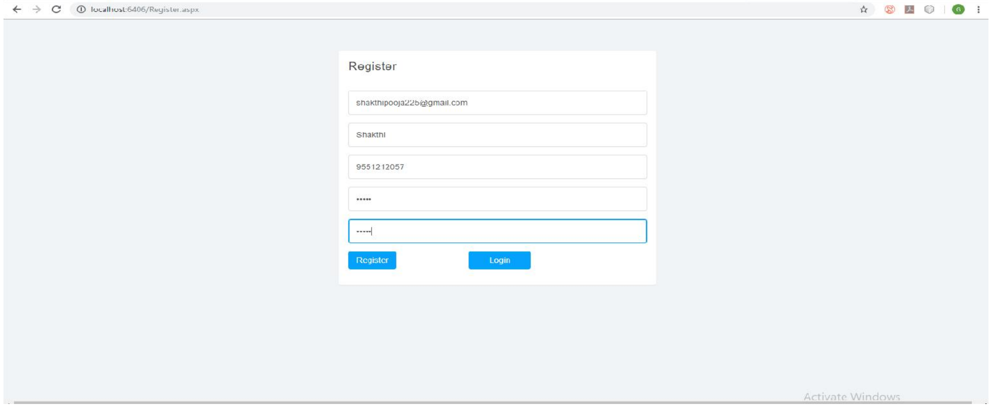


Fig-2: HOME PAGE



shakthipooja22b@gmail.com

Shakthi

9551212057

•••••

•••••

Fig-3: REGISTRATION PAGE

Fig-4: LOGIN PAGE

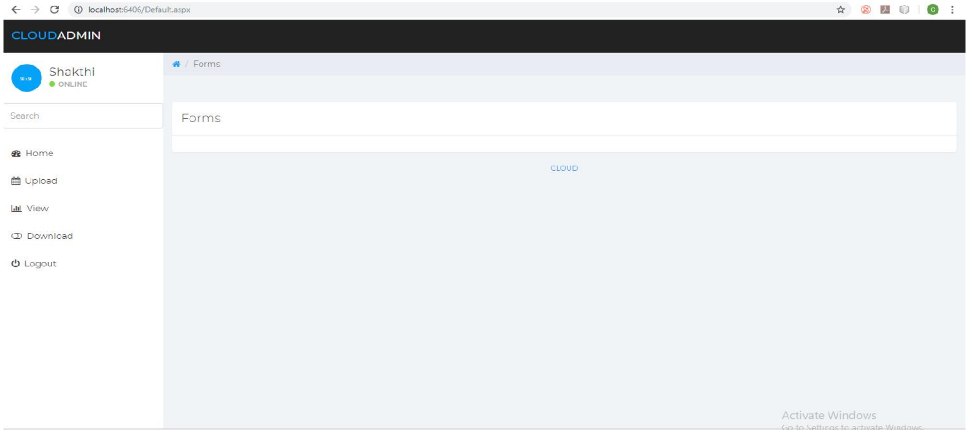


Fig-5: USER LOGIN PAGE

DOI: 10.48175/IJARSCT-4447

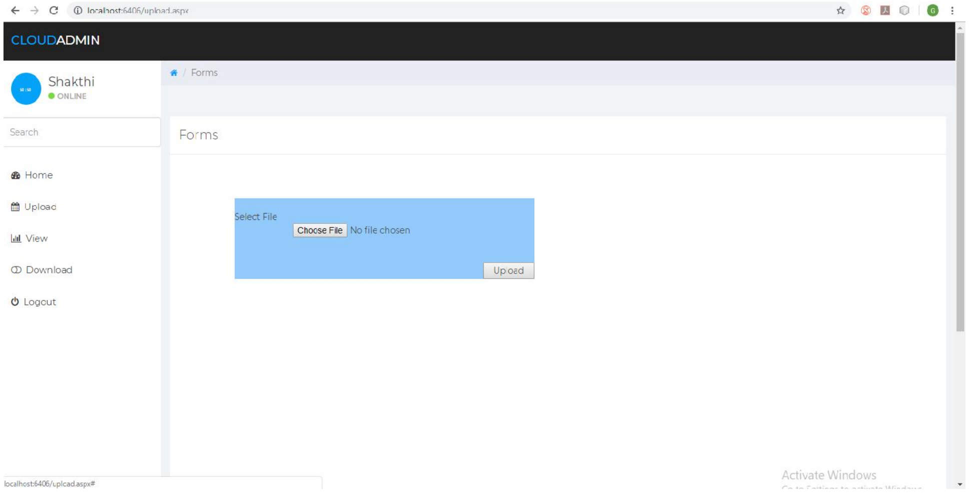
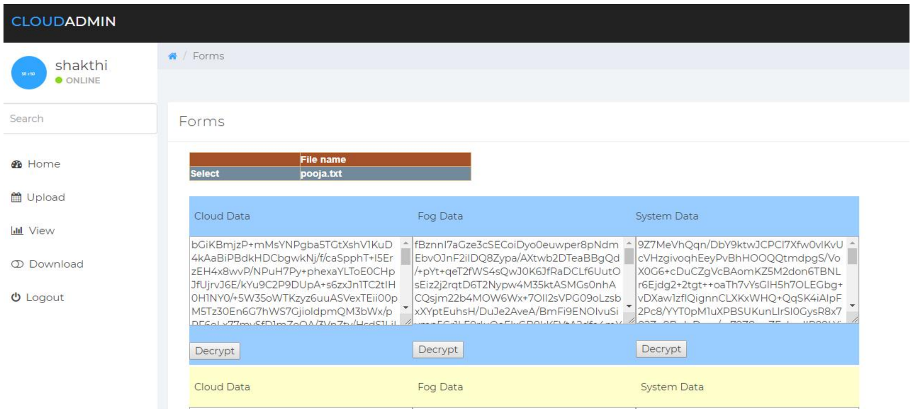


Fig-6: FILE UPLOAD

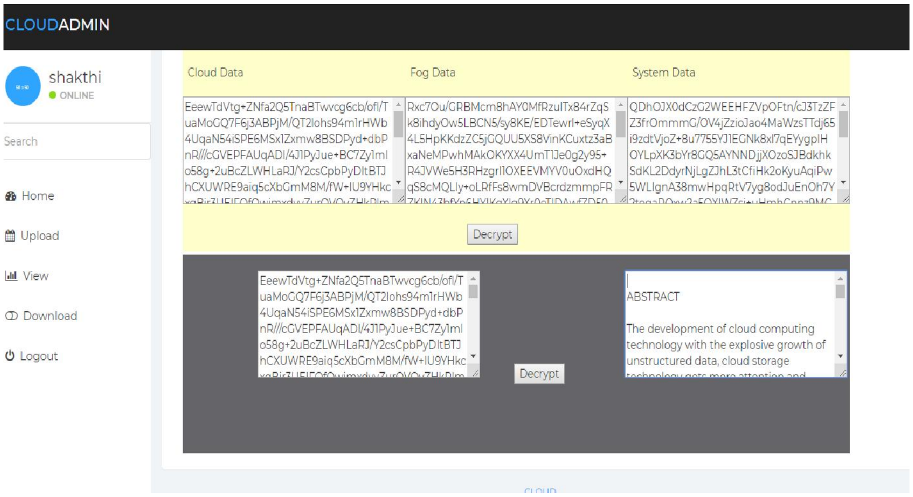


	File name
Select	pooja.txt

Cloud Data	Fog Data	System Data
bGiKBmjzP+mMsYNPgba5TGtXshV1KuD 4kAaBiPBdkHDCbgwkNj/f/caSpphT+I5Er zEH4x8wvP/NPuH7Py+phexaYLToE0CHp JfUjrvJ6E/kYu9C2P9DUpA+s6zxJn1TC2tIH 0H1NY0/+5W35oWTKzyz6uuASVexTEii00p M5Tz30En6G7hWS7GjioldpmQM3bWx/p	fBznnI7aGze3cSECoiDyo0euwper8pNdm EbvOJnF2iIDQ8Zypa/AXtwb2DTeaBBgQd /+pYt+qeT2fWS4sQwJ0K6JfRaDCLf6UutO sEiz2j2rqtD6T2Nypw4M35ktASMGs0nhA CQsjm22b4MOW6Wx+7OlI2sVPG09oLzsb xXYptEuhsH/DuJe2AveA/BmFi9ENOIvuSi	9Z7MeVhQqn/DbY9ktwJCPCI7Xfw0vIKvU cVHzgivoqhEeyPvBhHOOQQtmdpgS/Vo X0G6+cDuCZgVcBAomKZ5M2don6TBNL r6Ejdg2+2tgt++oaTh7vYsGIH5h7OLEGbg+ vDXaw1zfIQignnCLXKxWHQ+QqSK4iAIpF 2Pc8/YYT0pM1uXPBSUKunLIrSI0GysR8x7

Cloud Data	Fog Data	System Data

Fig-7: STORAGE SCHEME



Cloud Data	Fog Data	System Data
EeewTdVtg+ZNfa2Q5TnaBTwvcg6cb/ofl/T uaMoGQ7F6j3ABPjM/QT2lohs94m1rHWb 4UqaN54iSPE6MSx1Zxmw8BSDPyd+dbP nR///cGVEPFAUqADI/4J1PyJue+BC7Zy1ml o58g+2uBcZLWHLaRJ/Y2csCpbPyDItBTJ hCXUWRE9aiq5cXbGmM8M/fW+IU9YHkc	Rxc7Ou/GRBMcm8hAY0MfRzuITx84rZqS k8ihdyOw5LBCN5/sy8KE/EDTewrl+eSyqX 4L5HpKKdzZC5jGQUU5XS8VinKCuxtz3aB xaNeMPwhMAkOKYXX4UmT1Je0g2y95+ R4JVWe5H3RHzgrl1OXEEVMYV0uOxdHQ qS8cMQLly+oLRfFs8wmDVBcrdzmmpFR	QDhOJX0dCzG2WEEHFZVpOFtn/cJ3TzZF Z3frOmmmG/OV4jZzioJao4MaWzsTTdj65 i9zdtVjoZ+8u7755YJ1EGNk8xI7qEYygpIH OYLpXK3bYr8GQ5AYNNDjjXOzoSJBdkhk SdKL2DdyrNjLgZJhL3tCfiHk2oKyuAqiPw 5WLIgnA38mwHpqRtV7yg8odJuEnOh7Y

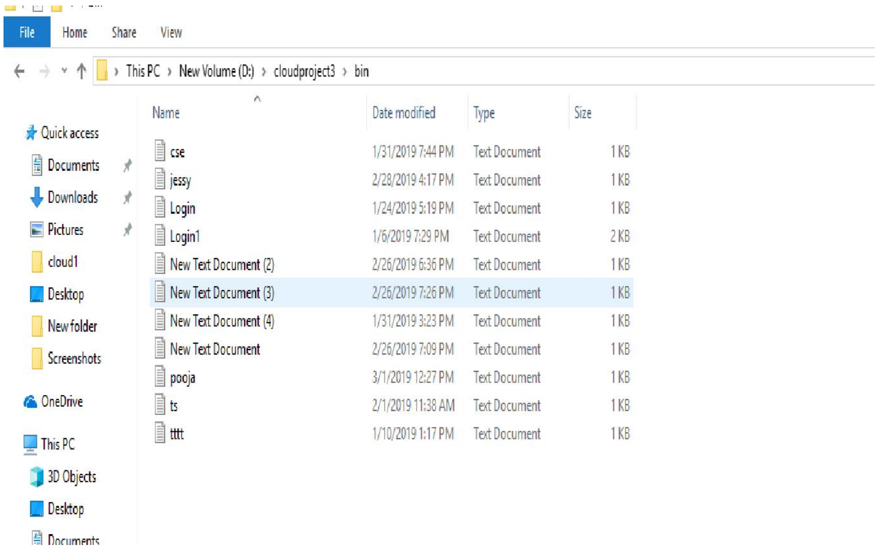
```
EeewTdVtg+ZNfa2Q5TnaBTwvcg6cb/ofl/T
uaMoGQ7F6j3ABPjM/QT2lohs94m1rHWb
4UqaN54iSPE6MSx1Zxmw8BSDPyd+dbP
nR///cGVEPFAUqADI/4J1PyJue+BC7Zy1ml
o58g+2uBcZLWHLaRJ/Y2csCpbPyDItBTJ
hCXUWRE9aiq5cXbGmM8M/fW+IU9YHkc
```

ABSTRACT

The development of cloud computing technology with the explosive growth of unstructured data, cloud storage

Fig-8: RECOVERY MODULE

DOI: 10.48175/IJARSCT-4447



Name	Date modified	Type	Size
cse	1/31/2019 7:44 PM	Text Document	1 KB
jessy	2/28/2019 4:17 PM	Text Document	1 KB
Login	1/24/2019 5:19 PM	Text Document	1 KB
Login1	1/6/2019 7:29 PM	Text Document	2 KB
New Text Document (2)	2/26/2019 6:36 PM	Text Document	1 KB
New Text Document (3)	2/26/2019 7:26 PM	Text Document	1 KB
New Text Document (4)	1/31/2019 3:23 PM	Text Document	1 KB
New Text Document	2/26/2019 7:09 PM	Text Document	1 KB
pooja	3/1/2019 12:27 PM	Text Document	1 KB
ts	2/1/2019 11:38 AM	Text Document	1 KB
tttt	1/10/2019 1:17 PM	Text Document	1 KB

Fig-9:BUCKET MODULE

VIII. ACKNOWLEDGMENT

We Would like to thank all our faculties, friends and family members who have directly and indirectly helped in easy completion of our project. Special thanks to Dr. M. Preetha, Professor, Department of Information Technology, Prince Shri Venkateshwara Padmavathy Engineering college, Chennai, Tamil Nadu, India for guiding us in completing this project successful.

REFERENCES

[1] P. Mell and T. Grance, “The NIST definition of cloud computing,” Nat.Inst. Stand. Technol., vol. 53, no. 6, pp. 50–50, 2009.

[2] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, “A survey of mobile cloudcomputing: Architecture, applications, and approaches,” Wireless Commun.Mobile Comput., vol. 13, no. 18, pp. 1587–1611, 2013.

[3] J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, “Joint virtual machine and bandwidth allocation in software defined network (sdn) and
cloud computing environments,” in Proc. IEEE Int. Conf. Commun., 2014,pp. 2969–2974.

[4] H. Li, W. Sun, F. Li, and B. Wang, “Secure and privacy-preserving datastorage service in public cloud,” J. Comput. Res. Develop., vol. 51, no. 7,
pp. 1397–1409, 2014.

[5] Y. Li, T.Wang, G.Wang, J. Liang, and H. Chen, “Efficient data collectionin sensor-cloud system with multiple mobile sinks,” in Proc. Adv. Serv.
Comput., 10th Asia-Pac. Serv. Comput. Conf., 2016, pp. 130–143.

[6] L. Xiao, Q. Li, and J. Liu, “Survey on secure cloud storage,” J. DataAcquis. Process., vol. 31, no. 3, pp. 464–472, 2016.

[7] R. J. McEliece and D. V. Sarwate, “On sharing secrets and reed-solomoncodes,” Commun. ACM, vol. 24, no. 9, pp. 583–584, 1981.

[8] J. S. Plank, “T1: Erasure codes for storage applications,” in Proc. 4th USENIX Conf. File Storage Technol., 2005, pp. 1–74.

[9] R. Kulkarni, A. Forster, and G. Venayagamoorthy, “Computational intelligence in wireless sensor networks: A survey,” IEEE Commun. Surv. Tuts.,vol. 13, no. 1, pp. 68–96, First Quarter 2011.

[10] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, “A privacypreserving and copy-deterrence content-based image retrieval scheme in
cloud computing,” IEEE Trans. Inf. Forensics Security, vol. 11, no. 11,pp. 2594–2608, Nov. 2016.

[11] J. Shen, D. Liu, J. Shen, Q. Liu, and X. Sun, “A secure cloud-assisted urban data sharing framework for ubiquitous-cities,” Pervasive Mobile
Comput., vol. 41, pp. 219–230, 2017.

[12] Z. Fu, F. Huang, K. Ren, J.Weng, and C.Wang, “Privacy-preserving smart semantic search based on conceptual graphs over encrypted outsourced data,” IEEE Trans. Inf. Forensics Security, vol. 12, no. 8, pp. 1874–1884,
Aug. 2017.

[13] J. Hou, C. Piao, and T. Fan, “Privacy preservation cloud storage architecture research,” J. Hebei Acad. Sci., vol. 30, no. 2, pp. 45–48, 2013.