BIBLIOGRAPHY

**BIBLIOGRAPHY**

**Referred Journals**

1. Z. Yan, L. F. Zhang, W. X. Ding, and Q. H. Zhen, “Heterogeneous data storage management with reduplication in cloud computing,” IEEE Transactions on Big Data, pp. 1–1, 2017.
2. Z. Yan, W. X. Ding, and H. Q. Zhu, “A scheme to manage encrypted data storage with deduplication in cloud,” in International Conference on Algorithms and Architectures for Parallel Processing, 2015.
3. Z. Yan, M. J. Wang, Y. X. Li, and A. V. Vasilakos, “Encrypted data

management with deduplication in cloud computing,” IEEE Cloud Computing, vol. 3, no. 2, pp. 28–35, 2016.

1. W. Shen, Y. Su, and R. Hao, “Lightweight cloud storage auditing with deduplication supporting strong privacy protection,” IEEE Access, vol. 8,

pp. 44 359–44 372, 2020.

1. Q. Zheng and S. Xu, “Secure and efficient proof of storage with

deduplication,” in CODASPY ’12, New York, NY, USA, 2012, p. 1–12.

1. A. Giuseppe, R. Burns, and C. Reza, “Provable data possession at untrusted stores,” in Proceedings of the 14th ACM Conference on Computer

and Communications Security, 2007, pp. 598–609.

1. G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, Z. Peterson, and D. Song, “Remote data checking using provable data possession,” ACM Transactions on Information and System Security, vol. 14, pp. 1– 34, 2011.
2. Z. Wen, J. Luo, H. Chen, J. Meng, X. Li, and J. Li, “A verifiable data deduplication scheme in cloud computing,” in INCOS ’14, USA, 2014,

p. 85–90.

1. P. Meye, P. Raïpin, F. Tronel, and E. Anceaume, “A secure two-phase

data deduplication scheme,” in HPCC ’14, CSS ’14, ICESS ’14, 2014,

pp. 802–809.

1. D. Vasilopoulos, M. Önen, K. Elkhiyaoui, and R. Molva, “Messagelocked proofs of retrievability with secure deduplication,” in Proceedings

of the 2016 ACM on Cloud Computing Security Workshop, 2016, pp. 73– 83.

1. M. Bellare, R. Canetti, and H. Krawczyk, “Keying hash functions for message authentication,” in CRYPTO ’96, Berlin, Heidelberg, 1996, pp. 1–15.
2. X. Q. Liang, Z. Yan, X. F. Chen, L. T. Yang, W. J. Lou, and Y. T. Hou,

“Game theoretical analysis on encrypted cloud data deduplication,” IEEE Transactions on Industrial Informatics, vol. 15, no. 10, pp. 5778–5789, 2019.

1. X. Q. Liang, Z. Yan, R. H. Deng, and Q. H. Zheng, “Investigating the adoption of hybrid encrypted cloud data deduplication with game theory,” IEEE Transactions on Parallel and Distributed Systems, vol. 32, no. 3,

pp. 587–600, 2021.

1. Z. Yan, W. Ding, X. Yu, H. Zhu, and R. H. Deng, “Deduplication on encrypted big data in cloud,” IEEE Transactions on Big Data, vol. 2,

no. 2, pp. 138–150, 2016.

1. A. Juels and B. S. Kaliski, “Pors: Proofs of retrievability for large files,”

in CCS ’07, New York, NY, USA, 2007, p. 584–597.

1. J. Xu and E.-C. Chang, “Towards efficient proofs of retrievability,” in Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, New York, NY, USA, 2012, p. 79–80.
2. C. M. Tang and X. J. Zhang, “A new publicly verifiable data possession

on remote storage,” Journal of supercomputing, vol. 75, no. 1, pp. 77–91, 2019.

1. H. Shacham and B. Waters, “Compact proofs of retrievability,” in ASIACRYPT ’08, Berlin, Heidelberg, 2008, pp. 90–107.
2. B. Dan, B. Lynn, and H. Shacham, “Short signatures from the weil pairing,” in ASIACRYPT ’01, 2001, pp. 514–532.
3. M. Azraoui, K. Elkhiyaoui, R. Molva, and M. Önen, “Stealthguard: Proofs of retrievability with hidden watchdogs,” in European Symposium on Research in Computer Security, 2014, pp. 39–256.
4. M. Bellare, S. Keelveedhi, and T. Ristenpart, “Message-locked encryption and secure deduplication,” in EUROCRYPT ’13, 2013, pp. 296–312.
5. A. Kate, G. M. Zaverucha, and I. Goldberg, “Constant-size commitments

to polynomials and their applications,” in ASIACRYPT ’10, 2010, pp. 177–194.

1. G. Wallace, F. Douglis, H. Qian, P. Shilane, and W. Hsu, “Characteristics

of backup workloads in production systems,” isn Proceedings of the 10th

USENIX conference on File and Storage Technologies, 2012, pp. 4–4.

1. R. Chen, Y. Mu, G. Yang, and F. Guo, “Bl-mle: Block-level messagelocked encryption for secure large file deduplication,” IEEE Transactions

on Information Forensics and Security, vol. 10, no. 12, pp. 2643–2652, 2015.

1. Y. Shin, J. Hur, and K. Kim, “Security weakness in the proof of storage

with deduplication,” Cryptology ePrint Archive, Report 2012/554, 2012,

https://eprint.iacr.org/2012/554.

1. A. Kiss, J. Liu, T. Schneider, N. Asokan, and B. Pinkas, “Private set intersection for unequal set sizes with mobile applications,” Proceedings of Privacy Enhancing Technologies, vol. 2017, no. 4, pp. 177–197, 2017.
2. E. D. Cristofaro and G. Tsudik, “Practical private set intersection protocols with linear complexity,” in Financial Cryptography and Data

Security, 2010, pp. 143–159.

1. E. Cristofaro and G. Tsudik, “Experimenting with fast private set intersection,” in Trust and Trustworthy Computing, Berlin, Heidelberg, 2012,

pp. 55–73.

1. B. Fan, D. G. Andersen, M. Kaminsky, and M. D. Mitzenmacher, “Cuckoo filter: Practically better than bloom,” in CoNEXT’14, 2014, pp. 77–85.
2. E. Kushilevitz and R. Ostrovsky, “Replication is not needed: single database, computationally-private information retrieval,” in Proceedings of the 38th Annual Symposium on Foundations of Computer Science, 1997, pp. 364–373

**APPENDIX – A**

**URL LISTING**

* + [www.google.co.in](http://www.google.co.in/)
  + [www.java.org](http://www.java.org/)
  + [www.w3schools.com](http://www.w3schools.com/)
  + [www.javatutorial.com](http://www.javatutorial.com/)

**REFERENCE BOOKS**

* Java Crash Course 2nd Edition - this is a basic level book for beginners.
* Learning java 5th Edition - this book is a practical learning book for basic to advanced level.
* Java Cookbook - this book for advanced programmer interested in learning about modern java development tools.
* Automating Boring Stuff With Java - In this book you will learn to write programs in java.
* Head First Java - this book covered the fundamental of java.
* Think Java - the basics of programming concepts and cover advanced topics like data structure and object-oriented design.

**APPENDIX – B**

* **GLOSSARY**
  + GUI : Graphical User Interface
  + UML : Unified Modeling Language
  + API : Application Programming Interface
  + HTML : Hyper Text Markup Language
  + URL : Uniform Resource Locator
  + ODBC : Open Database Connectivity

**APPENDIX – C**

* **List of Figures**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S.No.** | **Fig No.** | **Description** | **Page No.** | **Chapter** |
| 1 | 2.2.1.1 | System architecturestate | 9 | SRS |
| 2 | 2.7.1 | Non-Functional Requirements | 15 | SRS |
| 3 | 2.7.2 | Spiral model | 19 | SRS |
| 4 | 3.1.1 | ER diagram | 27 | System design |
| 5 | 3.3.1 | Use case diagram | 41 | System design |
| 6 | 3.3.2 | Class diagram | 41 | System design |
| 7 | 3.3.3 | Collaboration diagram | 42 | System design |
| 8 | 3.3.4 | Sequence diagram | 43 | System design |
| 9 | 3.3.5 | Activity Diagram | 44 | System design |
| 10 | 3.3.6 | State chart diagram | 44 | System design |
| 12 | 3.3.7 | Component Diagram | 45 | System design |
| 13 | 3.3.8 | Deployment Diagram | 45 | System design |
| 14 | 3.3.9 | Use case diagram | 46 | System design |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 15 | 3.3.10 | Class diagram | 47 | System design |
| 16 | 3.3.11 | Sequence diagram | 48 | System design |
| 17 | 3.3.12 | Activity Diagram | 49 | System design |
| 18 | 3.3.13 | Deployment Diagram | 50 | System design |

* **list of Tables**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S.**  **No** | **Table No** | **Table Name** | **Page No.** | **Chapter** |
| 1 | 3.2.1 | Data owner | 28 | System  design |
| 2 | 3.2.2 | Cloud service provider | 28 | System  design |
| 3 | 3.2.3 | Key generator | 29 | System  design |
| 4 | 3.2.4 | Third party auditor | 29 | System  design |
| 5 | 4.2.1 | Test cases | 54 | Testing |

* **List of screens**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S.**  **No.** | **ScreenN o.** | **ScreenName** | **Page No.** | **Chapter** |
| 1 | 5.1.1 | Working for java  program | **57** | Implementation |
| 2 | 5.1.2 | Implementation of java virtual machine | **58** | Implementation |
| 3 | 5.1.3 | Program running on the  java platform | **58** | Implementation |
| 4 | 5.1.4 | Properties wizard | **60** | Implementation |
| 5 | 5.1.5 | Path setting for java | **60** | Implementation |
| 6 | 5.1.6 | Welcome page of  tomcat of | **61** | Implementation |
| 6 | 5.1.7 | Tomcat configuration  option page | **62** | Implementation |
| 7 | 5.1.8 | Tomcat license  agreement | **63** | Implementation |
| 8 | 5.1.9 | Welcome wizard of my  sql | **64** | Implementation |
| 9 | 5.1.10 | Sql setup wizard | **64** | Implementation |
| 10 | 5.1.11 | Database configuration  engine | **65** | Implementation |
| 11 | 5.2.1 | Home page | **66** | Implementation |
| 12 | 5.2.2 | C;oud service provider | **67** | Implementation |
| 13 | 5.2.3 | Menu page | **68** | Implementation |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 14 | 5.2.4 | View all users | **69** | Implementation |
| 15 | 5.2.5 | Key generator | **70** | Implementation |
| 16 | 5.2.6 | tpa | **71** | Implementation |
| 17 | 5.2.7 | Data owner | **72** | Implementation |
| 18 | 5.2.8 | Registration | **73** | Implementation |
| 19 | 5.2.9 | My files | **74** | Implementation |
| 20 | 5.2.10 | Data owner registration | **75** | Implementation |
| 21 | 5.2.11 | Registration successfully | **76** | Implementation |
| 22 | 5.2.12 | Data owner login | **77** | Implementation |
| 23 | 5.2.13 | welcome | **78** | Implementation |
| 24 | 5.2.14 | Welcome to key generator | **79** | Implementation |
| 25 | 5.2.15 | To verify the data | **80** | Implementation |
| 26 | 5.2.16 | Upload data | **81** | Implementation |
| 27 | 5.2.17 | My files | **82** | Implementation |
| 28 | 5.2.18 | Upload daata | **83** | Implementation |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 29 | 5.2.19 | Upload data | **84** | Implementation |
| 30 | 5.2.20 | Upload data sucess | **85** | Implementation |
| 31 | 5.2.21 | Search file | **86** | Implementation |
| 32 | 5.2.22 | View file | **87** | Implementation |
| 33 | 5.2.23 | Request key | **88** | Implementation |
| 34 | 5.2.24 | Download | **89** | Implementation |
| 35 | 5.2.25 | Verify file | **90** | Implementation |
| 36 | 5.2.26 | Send to tpa | **91** | Implementation |
| 37 | 5.1.27 | To receive the tpa | **92** | Implementation |
| 38 | 5.1.28 | Send to server for verify file | **93** | Implementation |
| 39 | 5.1.29 | Send to server for verification | **94** | Implementation |
| 40 | 5.1.30 | View all files | **95** | Implementation |
| 41 | 5.1.31 | Verify files in cloud server | **96** | Implementation |
| 42 | 5.1.32 | To check files is safe | **97** | Implementation |
| 43 | 5.1.33 | Send to owner | **98** | Implementation |
| 44 | 5.1.34 | Send to data owner | **99** | Implementation |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 45 | 5.1.35 | verification | **100** | Implementation |
| 46 | 5.1.36 | verify | **101** | Implementation |
| 47 | 5.1.37 | Verify file status | **102** | Implementation |