No.	Topic	Research	Technology	How	Results	Future Scope
1	Data Security and Privacy Protection for Cloud Storage	1.One to Many Encryption 2.Data Integrity 3.Data Deletion 4.Leakage-Resilient 5.Privacy Preserving	1.Identity Based Encryption 2.Attribute based Encryption 3.Homomorphic Encryption 4.Searchable Encryption	1.Privacy Preserving and Machine Learning in cloud 2.Post Quantum Encryption	Introduce the encryption principles of IBE, ABE, homomorphic encryption, searchable encryption and the research direction of new encryption models.	Data encryption technologies and protection methods these correspond to the mentioned security requirements
2	Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage	1.Frameworks - KeyGen, Encrypt, Extract, Decrypt 2.Sharing Encrypted Data	1.Cryptographic Keys for a Predefined Hierarchy 2.Compact Key in Symmetric-Key Encryption 3.Compact Key in Identity-Based Encryption	1.Public-Key Extension 2.Compression Factors	How to “compress” secret keys in public-key cryptosystems which support delegation of secret keys for different ciphertext classes in cloud storage.	Designing a leakage-resilient cryptosystem yet allows efficient and flexible key delegation is also an interesting direction.

No.	Topic	Research	Technology	How	Results	Future Scope
3	Achieving Secure Role-based Access Control on Encrypted Data in Cloud Storage	1.Role-based Encryption Systems 2.The Bilinear Pairings	1.Role-based Encryption schema Construction - Setup, Extract, Manage Role, Add User, Encrypt, Decrypt, Revoke User	1.Architectural Components 2.System Operations	Encryption and decryption computations are efficient on the client side, and decryption time at the cloud can be reduced by having multiple processors, which is common in a cloud environment.	Useful in commercial situations as it captures practical access policies based on roles in a flexible manner and provides secure data storage in the cloud enforcing these access policies.
4	A Cost-effective Dynamic Replication Management Scheme for Cloud Storage Cluster	1.CloudStorage 2.DataReplication 3.Replica Placement 4.Cost Effective 5.Dynamic Replication Management	1.System Model 2.Availability - Node Available, Node Unavailable, Block Available, Block Unavailable, File Available, File Unavailable 3.Blocking Probability	1.Implementation in HDFS 2.Control Strategies 3.Load Balance	CDRM further places replicas among cloud nodes to minimize blocking probability, so as to improve load balance and overall performance.	Maintains a rational number of replica, which not only satisfies availability, but also improves access latency, load balance, and keeps the whole storage system stable.

No.	Topic	Research	Technology	How	Results	Future Scope
5	Privacy-Preserving Public Auditing for Secure Cloud Storage	1.The System and Threat Model 2.Design Goals	1.MAC-based Solution. 2.Privacy-Preserving Public Auditing Scheme 3.Security Guarantee for Batch Auditing 4.Cost of Privacy-Preserving Protocol	1.Support for Batch Auditing 2.TPA 3.Cloud Server 4.Storage Correctness Guarantee 5.Generalization	Eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage.	Extend our privacy-preserving public auditing protocol into a multi-user setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency.
6	Combining Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage	1.Ciphertext-Policy Attribute-Based-Encryption 2.Authenticated Encryption With Associated Data 3.Digital Signature 4.Hybrid Encryption for CP-ABE 5.Bloom Filter 6.Building Systems Against Covert Adversaries	1.System Model 2.data owners, data users, and the cloud provider.	1.Partially Outsourced Protocol (POP) 2.Fully Outsourced Protocol (FOP) 3.Security Against EDoS Attacks	Bloom filter and probabilistic check in the resource consumption accounting to reduce the overhead.	Performance analysis shows that the overhead of our construction is small over existing systems.

No.	Topic	Research	Technology	How	Results	Future Scope
7	Enabling Cloud Storage Auditing with Key-Exposure Resistance	1.System model 2.Security Model-Setup Phase, Query Phase, Break-in Phase, Forgery Phase	1.Naive 2.Cloud Storage Auditing with Key-exposure Resilience	1.Support the TPA 2.Support lazy update 3.Support multiple sectors	1.propose a new paradigm called auditing protocol with key-exposure re-silience. 2.the security model of auditing protocol with key-exposure resilience, and then propose the first practical solution.	The security proof and the asymptotic performance evaluation show that the proposed protocol is secure and efficient.
8	Dual-server public-key encryption with keyword Search for secure cloud storage	1.KeyGen, DS−PEKS, DS−Trapdoor,FrontTest,BackTest 2.Security Models	1.SPHFSetup, HashKG, ProjKG,Hash, ProjHash 2.New Variant–Linear and Homomorphic SPHFs	1.Semantic-Security Against Chosen Keyword Attack. 2.Indistinguishability Against Keyword Guessing Attack. 3.Semantic-Security Against Chosen Keyword Attack.	1.Prevent the inside keyword guessing attack which is an inherent vulnerability of the traditional PEKS framework. 2.Smooth Projec- tive Hash Function (SPHF)	An efficient instantiation of the new SPHF based on the Diffie-Hellman problem is also presented in the paper, which gives an efficient DS-PEKS scheme without pairings.