**LITERATURE SURVEY**

**[1] Alexandros Bakas and Antonis Michalas. Modern family: A revocable hybrid encryption scheme based on attribute-based encryption, symmetric searchable encryption and SGX. In SecureComm 2019, pages 472–486, 2019.**

Secure cloud storage is considered as one of the most important issues that both businesses and end-users take into account before moving their private data to the cloud. Lately, we have seen some interesting approaches that are based either on the promising concept of Symmetric Searchable Encryption (SSE) or on the well-studied field of Attribute-Based Encryption (ABE). In this paper, we propose a hybrid encryption scheme that combines both SSE and ABE by utilizing the advantages of both these techniques. In contrast to many approaches, we design a revocation mechanism that is completely separated from the ABE scheme and solely based on the functionality offered by SGX

**[2] Antonis Michalas. The lord of the shares: combining attributebased encryption and searchable encryption for ﬂexible data sharing. In SAC 2019, pages 146–155, 2019**

Secure cloud storage is considered one of the most important issues that both businesses and end-users are considering before moving their private data to the cloud. Lately, we have seen some interesting approaches that are based either on the promising concept of Symmetric Searchable Encryption (SSE) or on the well-studied field of Attribute-Based Encryption (ABE). In the first case, researchers are trying to design protocols where users' data will be protected from both *internal* and *external* attacks without paying the necessary attention to the problem of user revocation. On the other hand, in the second case existing approaches address the problem of revocation. However, the overall efficiency of these systems is compromised since the proposed protocols are solely based on ABE schemes and the size of the produced ciphertexts and the time required to decrypt grows with the complexity of the access formula. In this paper, we propose a protocol that combines *both* SSE and ABE in a way that the main advantages of each scheme are used. The proposed protocol allows users to directly search over encrypted data by using an SSE scheme while the corresponding symmetric key that is needed for the decryption is protected via a Ciphertext-Policy Attribute-Based Encryption scheme.

**[3] G. Wang, C. Liu, Y. Dong, P. Han, H. Pan, and B. Fang, “Idcrypt: A multi-user searchable symmetric encryption scheme for cloud applications,” IEEE Access, vol. 6, pp. 2908–2921, 2018.**

Searchable Encryption (SE) has been extensively examined by both academic and industry researchers. While many academic SE schemes show provable security, they usually expose some query information (e.g., search and access patterns) to achieve high efficiency. However, several inference attacks have exploited such leakage, e.g., a query recovery attack can convert opaque query trapdoors to their corresponding keywords based on some prior knowledge. On the other hand, many proposed SE schemes require significant modification of existing applications, which makes them less practical, weak in usability, and difficult to deploy. In this paper, we introduce a secure and practical searchable symmetric encryption scheme with provable security strength for cloud applications, called IDCrypt, which improves the search efficiency, and enhances the security strength of SE using symmetric cryptography. We further point out the main challenges in securely searching on multiple indexes and sharing encrypted data between multiple users. To address the above issues, we propose a token-adjustment search scheme to preserve the search functionality among multi-indexes, and a key sharing scheme which combines identity-based encryption and public-key encryption. Our experimental results show that the overhead of the key sharing scheme is fairly low.

**[4] Kaiping Xue, Weikeng Chen, Wei Li, Jianan Hong, and Peilin Hong. Combining data owner-side and cloud-side access control for encrypted cloud storage. IEEE Transactions on Information Forensics and Security, 2018.**

People endorse the great power of cloud computing, but cannot fully trust the cloud providers to host privacy-sensitive data, due to the absence of user-to-cloud controllability. To ensure confidentiality, data owners outsource encrypted data instead of plaintexts. To share the encrypted files with other users, ciphertext-policy attribute-based encryption (CP-ABE) can be utilized to conduct fine-grained and owner-centric access control. But this does not sufficiently become secure against other attacks. Many previous schemes did not grant the cloud provider the capability to verify whether a downloader can decrypt. Therefore, these files should be available to everyone accessible to the cloud storage. A malicious attacker can download thousands of files to launch economic denial of sustainability (EDoS) attacks, which will largely consume the cloud resource. The payer of the cloud service bears the expense. Besides, the cloud provider serves both as the accountant and the payee of resource consumption fee, lacking the transparency to data owners. These concerns should be resolved in real-world public cloud storage. In this paper, we propose a solution to secure encrypted cloud storages from EDoS attacks and provide resource consumption accountability. It uses CP-ABE schemes in a black-box manner and complies with arbitrary access policy of the CP-ABE. We present two protocols for different settings, followed by performance and security analysis

**[5] Jianting Ning, Zhenfu Cao, Xiaolei Dong, Kaitai Liang, Hui Ma, and Lifei Wei. Auditable σ-time outsourced attribute-based encryption for access control in cloud computing. IEEE Transactions on Information Forensics and Security, 13(1):94–105, 2018..**

As a sophisticated mechanism for secure finegrained access control over encrypted data, ciphertext-policy attribute-based encryption (CP-ABE) is one of the highly promising candidates for cloud computing applications. However, there exist two main long-lasting open problems of CP-ABE that may limit its wide deployment in commercial applications. One is that decryption yields expensive pairing cost which often grows with the increase of access policy size. The other is that one is granted access privilege for unlimited times as long as his attribute set satisfies the access policy of a given ciphertext. Such powerful access rights, which are provided by CP-ABE, may be undesirable in real-world applications (e.g., pay-as-youuse). To address the above drawbacks, in this paper, we propose a new notion called auditable σ-time outsourced CF-ABE, which is believed to be applicable to cloud computing. In our notion, expensive pairing operation incurred by decryption is offloaded to cloud and meanwhile, the correctness of the operation can be audited efficiently. Moreover, the notion provides σ-time fine-grained access control. The cloud service provider may limit a particular set of users to enjoy access privilege for at most σ times within a specified period. As of independent interest, the notion also captures key-leakage resistance. The leakage of a user's decryption key does not help a malicious third party in decrypting the ciphertexts belonging to the user. We design a concrete construction (satisfying our notion) in the key encapsulation mechanism setting based on Rouselakis and Waters (prime order) CP-ABE, and further present security and extensive experimental analysis to highlight the scalability and efficiency of our construction