**LITERATURE SURVEY**

**Title:** Ciphertext-policy attribute-based encryption.

**Abstract:** In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call ciphertext-policy attribute-based encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous attribute-based encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as role-based access control (RBAC). In addition, we provide an implementation of our system and give performance measurements.

**Title:** Innovative technology for cpu based attestation and sealing.

**Abstract:** Intel is developing the Intel® Software Guard Extensions (Intel® SGX) technology, an extension to Intel® Architecture for generating protected software containers. The container is referred to as an enclave. Inside the enclave, software’s code, data, and stack are protected by hardware enforced access control policies that prevent attacks against the enclave’s content. In an era where software and services are deployed over the Internet, it is critical to be able to securely provision enclaves remotely, over the wire or air, to know with confidence that the secrets are protected and to be able to save secrets in non-volatile memory for future use. This paper describes the technology components that allow provisioning of secrets to an enclave. These components include a method to generate a hardware based attestation of the software running inside an enclave and a means for enclave software to seal secrets and export them outside of the enclave (for example store them in non-volatile memory) such that only the same enclave software would be able un-seal them back to their original form.

**Title:**  A revocable hybrid encryption scheme based on attribute-based encryption, symmetric searchable encryption and SGX

**Abstract:** 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.

**Title:** Secure schemes for secret sharing and key distribution

**Abstract:** In recent years the security of operations taking place over a computer network become very important. It is necessary to protect such actions against \bad" users who may try to misuse the system (e.g. steal credit card numbers, execute actions without authorization, read personal mail, or impersonate other users). Many cryptographic protocols and schemes were designed to solve problems of this type. This thesis deals with two fundamental cryptographic tools that are useful in such contexts: generalized secret sharing schemes, and key distribution schemes.

**Title:** Dan Boneh, and Sergey Gorbunov. IRON: functional encryption using intel SGX.

**Abstract:** Functional encryption (FE) is an extremely powerful cryptographic mechanism that lets an authorized entity compute on encrypted data, and learn the results in the clear. However, all current cryptographic instantiations for general FE are too impractical to be implemented. We construct IRON, a provably secure, and practical FE system using Intel's recent Software Guard Extensions (SGX). We show that IRON can be applied to complex functionalities, and even for simple functions, outperforms the best known cryptographic schemes. We argue security by modeling FE in the context of hardware elements, and prove that IRON satisfies the security model.

**Title:** Secure integration of asymmetric and symmetric encryption schemes.

**Abstract:** This paper presents a generic conversion from weak asymmetric and symmetric encryption schemes to an asymmetric encryption scheme that is chosen-ciphertext secure in the random oracle model. Our conversion is the first generic transformation from an arbitrary one-way asymmetric encryption scheme to a chosen-ciphertext secure asymmetric encryption scheme in the random oracle model.

**Title:** Attribute-based encryption for fine-grained access control of encrypted data

**Abstract:** As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. We demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

**Title:** Improving privacy and security in decentralized ciphertext-policy attribute-based encryption

**Abstract:** In previous privacy-preserving multiauthority attribute-based encryption (PPMA-ABE) schemes, a user can acquire secret keys from multiple authorities with them knowing his/her attributes and furthermore, a central authority is required. Notably, a user's identity information can be extracted from his/her some sensitive attributes. Hence, existing PPMA-ABE schemes cannot fully protect users' privacy as multiple authorities can collaborate to identify a user by collecting and analyzing his attributes. Moreover, ciphertext-policy ABE (CP-ABE) is a more efficient public-key encryption, where the encryptor can select flexible access structures to encrypt messages. Therefore, a challenging and important work is to construct a PPMA-ABE scheme where there is no necessity of having the central authority and furthermore, both the identifiers and the attributes can be protected to be known by the authorities. In this paper, a privacy-preserving decentralized CP-ABE (PPDCP-ABE) is proposed to reduce the trust on the central authority and protect users' privacy. In our PPDCP-ABE scheme, each authority can work independently without any collaboration to initial the system and issue secret keys to users. Furthermore, a user can obtain secret keys from multiple authorities without them knowing anything about his global identifier and attributes.

**Title:** Attribution of fraudulent resource consumption in the cloud.

**Abstract:** Obligated by a utility pricing model, Internet-facing web resources hosted in the public cloud are vulnerable to Fraudulent Resource Consumption (FRC) attacks. Unlike an application-layer DDoS attack that consumes resources with the goal of disrupting short-term availability, an FRC attack is a considerably more subtle attack that instead seeks to disrupt the long-term financial viability of operating in the cloud by exploiting the utility pricing model over an extended time period. By fraudulently consuming web resources in sufficient volume (i.e. data transferred out of the cloud), an attacker (e.g. botnet) is able to incur significant fraudulent charges to the victim. This paper proposes an attribution methodology to identify malicious clients participating in an FRC attack. Experimental results demonstrate that the presented methodology achieves qualified success against challenging attack scenarios.

**Title:** . Intel R software guard extensions: Epid provisioning and attestation services

**Abstract:** Gramine project uses [SGX](https://gramine.readthedocs.io/en/stable/glossary.html#term-sgx) to securely run software. SGX is a complicated topic, which may be hard to learn, because the documentation is scattered through official/reference documentation, blogposts and academic papers. This page is an attempt to curate a dossier of available reading material.