Kui Ren

Assistant Professor
Email: kren2@iit.edu

Ubiquitous Security & Privacy Research Laboratory (UbiSeC Lab)
Department of Electrical and Computer Engineering
Illinois Institute of Technology
3301 S Dearborn St., Siegel Hall 319
Chicago, Illinois 60616

My research interests lie in the general area of cloud computing security, with current emphasis on secure and privacy assured data service outsourcing in cloud computing. The two topics that best fit my research interests are the following: 1) Cloud Security, Privacy, and Auditing; 2) Data Portability, Consistency, and Management.

The research projects that I am now actively pursuing related to Cloud Computing are summarized below:

Cloud Computing economically enables a fundamental paradigm shift on how data services are deployed and delivered, i.e., enabling service outsourcing, where individual and enterprise customers can avoid committing large capital outlays in the purchase and management of both software and hardware and the operational overhead therein. Despite the tremendous benefits, outsourcing data service to the commercial public cloud is also depriving customers' direct control over the systems that manage their data, raising security and privacy as the primary obstacles to the adoption of the cloud. Addressing these security challenges thus becomes the key to the success of deploying the most fundamental data services including data storage, data sharing, and data utilization on the commercial public cloud.

1) **Privacy-preserving Secure Cloud Storage Auditing**. This research investigates how to outsource storage service in cloud while maintaining strong storage correctness guarantee, given the challenge that data are no longer locally possessed by the data owners. Techniques are developed to enable public auditing for outsourced cloud data, which allows a third-party auditor to perform on-demand privacy-preserving storage correctness auditing, without introducing any additional on-line burden to the data owner, or new vulnerabilities towards owners' data privacy. For practical storage auditing service deployment, techniques are also developed to support fully dynamic data operations and efficient batch auditing, while satisfying the requirements of storage correctness protection.

2) **Scalable and Owner-Controller Cloud Data Sharing**. This research investigates owner-controlled cloud data sharing service with fine-grained data access enforcement and system scalability, given the challenge that cloud data no longer resides on owners' trusted domain but in a large scale dynamic system with frequent user access privilege updates. In order to minimize the management and online burden towards the data owner for the overall data access enforcement, techniques are developed to enable data owners to securely leverage the computation resource richness of the cloud. As a result, most cumbersome key/data management workload, e.g. for frequent user access privilege update, can be delegated to cloud without compromising data confidentiality, thus achieving a scalable design.

These research projects are partially supported through **Amazon Web Service research** and to be funded by **NSF Career Award**. For further information, please see the project web site at: http://www.ece.iit.edu/~ubisec/cloud/

Future Research:

1) **Privacy-assured and Effective Cloud Data Utilization**. As the data produced by enterprises and individuals that need to be stored and utilized is rapidly increasing, data owners are motivated to outsource their local complex data management systems into the cloud for its great flexibility and economic savings. To protect data privacy and combat unsolicited accesses in cloud and beyond, sensitive data has to be encrypted before outsourcing; this, however, obsoletes the traditional data utilization service based on plaintext keyword search. Thus, enabling an encrypted cloud data search service with privacy-assurance is of paramount importance. Considering the potentially large number of on-demand data users and huge amount of outsourced data files in the cloud, this problem is particularly challenging, as it is extremely difficult to meet also the requirements of performance, system usability and scalability. This research project aims to explore such a privacy-assured and effective cloud data utilization service with high service-level performance and usability, by investigating the two challenging research tasks: fuzzy keyword search and ranked keyword search over encrypted cloud data. Fuzzy keyword search, opposing to exact keyword match, tolerates minor typos and format inconsistencies in user search request, and greatly enhances system usability and user searching experience. Its challenge lies in the fact that two words similar to each other would no longer be so after one-way cryptographic transformation (for encrypted keyword search). To address the problem, we plan to explore a brand new symbol-based trie-traverse searching approach, in which transformed fuzzy keywords extracted from data files are stored using a multi-way tree structure to support efficient search, while protecting keyword privacy. Ranked keyword search further ensures the file retrieval accuracy and allows the user to find the most/least relevant information efficiently. We plan to explore the statistical measure approach (i.e. relevance score) from information retrieval (IR), and properly hide the scores in an order-preserved manner. The resulting design is expected to facilitate efficient server-side ranking without losing keyword privacy. For practical performance, different system parameters and the corresponding security/efficiency tradeoff are yet to be investigated. This research project is to be funded by **NSF CAREER Award**, starting from 2011.

2) **Engineering Secure Data Computation Outsourcing in Cloud Computing**. A fundamental concern to move computational workloads from private resources to the cloud is the protection of the confidential data that the computation consumes and produces. Thus, secure computation outsourcing mechanisms are in great need to not only protect sensitive workload information but validate the integrity of the computation result. This is, however, a very difficult task due to a number of challenges that have to be met simultaneously. Firstly, such a mechanism has to be practically feasible in terms of computational complexity. Secondly, it has to provide sound security guarantee without restricted system assumptions. Thirdly, it also has to enable substantial computational savings at the end-user's side as compared to the amount of the efforts that otherwise has to be committed to solve the problem locally. These challenges practically exclude the applicability of the existing techniques developed in the context of secure multi-party computation and fully homomorphic encryption. This research project proposes to study secure computation outsourcing in cloud computing with the above challenges in mind. We plan to focus on widely applicable engineering computing and optimization problems. We plan to study the methodology to explicitly decompose computations into public programs and private data and leverage the structures of specific computations for achieving desirable trade-offs among security, efficiency, and practicality. We propose to organize the mechanisms into a hierarchy where computation can be represented at various abstraction levels, such that the aforementioned trade-offs can be flexibly explored in a systematic manner. Two critical applications to be studied in this project include secure outsourcing systems of linear equations (LE) and secure outsourcing linear programming (LP) in the cloud. These two applications are among the most widely used algorithmic and computational tools in various engineering disciplines that analyze and optimize real-world systems. The study would prepare a solid knowledge base and provide insights for further research on more advanced computation problems, such as secure outsourcing convex programming in cloud. Prototype systems are to be built on the Amazon cloud platforms to validate the effectiveness of the proposed approach applying to various engineering computing and optimization problems. Some preliminary result of this project on secure outsourcing LP in cloud is going to appear at IEEE INFOCOM 2011.