The major concern in data application security is to specify the security requirements for data-centric applications, and design information systems that meet the security requirements.

An emerging idea in our research is to conduct empirical analysis on real-world data for better prediction or management of information security technology. Another idea is to embed user identification information into data for ownership protection or tamper detection.

An emerging idea in our research is to conduct empirical analysis on real-world data for better prediction or management of information security technology. Another idea is to embed user identification information into data for ownership protection or tamper detection.

Empirical analysis on market data of adopting information security technology such as trusted computing shows that traditional two-factor diffusion model based on influentials and imitators should be extended to include the effect of opponents as the third factor for better prediction of technology diffusions. Based on the distribution of public key certificate revocations discovered from real data, optimal strategies are devised for certificate authorities to manage certificate revocation lists in a cost-effective manner.

A series of rights management techniques are designed for protecting numerical (non-multimedia) data sets. These techniques include robust watermarking, fragile watermarking, public watermarking, multiple watermarking, and collusion resistant fingerprinting, while the data sets being protected include relational data, categorical data, data cubes, and data streams. These techniques can be effectively used for ownership proving and traitor tracing in data distributions in the presence of attacks such as tuple/attribute insertion/deletion, random/selective value modification, data frame-up, and additional watermark/fingerprint insertion.