Abstract

Advancement in network technology has presented a scalable platform for digital content trade. However, it is easy to copy and redistribute the digital content over the network without any quality degradation, which causes rampant piracy. Digital rights management (DRM) systems emerge as an effective solution to resist digital content piracy. These systems try to protect copyrights of content providers by restricting the illegal distribution.

The DRM systems adopts various technique, tools and policies to achieve persistence access control on the sold digital content to ensure copyright protection. They mostly focussed on the merchant concerns such as content security, persistence access control, copyright protection, traitor tracing, data collection, etc. In other words, most of the DRM systems are merchant centric and they either ignored or poorly addressed consumers' concerns. A consumer always wishes an user-friendly content access environment where he can easily access the content and play on any of his desirable devices without loosing the privacy. Although these basic requirements are not properly addressed, as a result consumers' privacy is always at risk and they are bound to play the digital content on the device content is locked or hardware configuration used for creating the digital license. These drawbacks unmotivated the adoption of DRM system and a user may wish to avoid the adoption of DRM systems which directly impact on the electronic commerce.

The main objective of this study is to address consumers' concerns and to propose some DRM models to address them. The proposed models discussed privacy and anonymity, user-friendliness, easy access, regionalism and portability. Moreover, the proposed schemes enhance the functionality requirement of content distribution, such as transparency, key management, location based content distribution. The presented study has two folds. In first part privacy issue is address with other relevant issues and portability issue is address in second part.

In the first part of the thesis discussed the privacy with other functionalities, such as a multi-distributor, key management, location dependent content distribution. Presented study address the and privacy issue in the following scenarios: license acquisition, content download, rights violation detection, data collection. We design a privacy preserving DRM scheme which is suitable for more innovative and scalable business models considering a network with multi-distributors instead of the single-distributor. The consumer has the flexibility of choosing a distributor based on his own preference. He may contact the distributor who is nearest to him by location or who offers promotions/discounts on the price or offers more commissions. The presented scheme facilitates privacy preserving, easy and accountable access of content. Moreover, the privacy protecting data collection and rights violation detection mechanism are addressed where system can collect the data of content sell and malicious consumer can be track without threatening the privacy of authorized consumers. We extend our work and proposed a privacy enhancing key management schemes in which encrypted digital content sent by the content provider can only be decrypted by the consumer who has a valid license and no one else without disclosing content identity to the involve principals. In addition, we propose a privacy preserving location dependent content distribution using multi-distributor based DRM model in which the distributors can help in handling different pricing structures of media in different countries.

The second part of study in this thesis is to investigate and develop portable DRM systems. We analyze some of the existing portable DRM schemes based on smart card and show their vulnerability to the most common attacks and inefficiency to satisfies desirable attributes. We a propose a password based authenticated key agreement scheme for portable DRM system using smart card which is an efficient and secure scheme protecting anonymity. We extend this work to achieve three factor authentication using consumer biometric identification in which only the authorized consumer who have access rights and permissions can access the content.

Keywords: Digital rights management; Content distribution; Anonymity; Privacy; Accountability; Key management; Portability.