Chapter 3
Anonymous Authentication for Privacy Preserving of Multimedia Data in the Cloud

Sadiq J. Almuairfi

https://orcid.org/0000-0002-7275-1677

Prince Sultan University, Saudi Arabia

Mamdouh Alenezi

https://orcid.org/0000-0001-6852-1206

Prince Sultan University, Saudi Arabia

ABSTRACT

Cloud computing technology provides cost-saving and flexibility of services for users. With the explosion of multimedia data, more and more data owners would outsource their personal multimedia data on the cloud. In the meantime, some computationally expensive tasks are also undertaken by cloud servers. However, the outsourced multimedia data and its applications may reveal the data owner's private information because the data owners lose control of their data. Recently, this thought has aroused new research interest on privacy-preserving reversible data hiding over outsourced multimedia data. Anonymous Authentication Scheme will be proposed in this chapter as the most relatable, applicable, and appropriate techniques to be adopted by the cloud computing professionals for the eradication of risks that have been associated with the risks and challenges of privacy.

INTRODUCTION

Authentication is a process of determining whether a particular individual or a device should be allowed to access a system or an application or merely an object running on a device. This is an important process which assures the basic security goals, viz. confidentiality and integrity. Also, adequate authentication is the first line of defence for protecting any resource. It is important that the same authentication technique may not be used in every scenario. For example, a less sophisticated approach may be used for accessing

a "chat server" compared to accessing a corporate database. Most of the existing authentication schemes require processing at both the client and the server end. Thus, the acceptability of any authentication scheme greatly depends on its robustness against attacks as well as its resource requirement both at the client and at the server end. The resource requirement has become a major factor due to the proliferation of mobile and hand-held devices. Nowadays, with the use of mobile phones, users can access any information including banking and corporate databases.

Anonymity is closely tied to confidentiality and privacy. A user should know that his online activity is secure and available only to him and a certain few authorized individuals from the service provider. That a user can have his entire browsing, purchasing activity accessed by others is unacceptable, and cloud service providers should ensure that this does not occur. Users should not have a fraudster accessing details of the online stores they visited, items purchased, frequency of visits and details of transactions.

The key to anonymity is the avoidance of the interception of the data being sent. If a user's cloud status cannot be ascertained, anonymity will be ensured, as third parties will not be able to tell whether a user is active or not, hence data interception will not occur. Users should have their anonymity guaranteed and no cookies should be allowed to monitor their activities, as cloud service deals with sensitive financial and personal data which could be used to detrimental ends if it fell into the wrong hands

Hiding one's real identity is important for users who do not like to share their personal or private information with others, for example, they may not want to share information regarding their meeting schedules with their business partners, which books they buy and read, how much money they have in their accounts, which transactions they execute, where they go, etc. In short, many users strongly prefer to remain anonymous as far as and whenever possible.

Since the revival of the 20th century, there is an enormous growth of mobile and wireless technologies. At present, a huge majority in the user of wireless devices, including mobile phones, for instance, notebooks, smartphones, PDAs, and so on, for accessing diverse online applications and services globally at any time. The services might include video conferencing, webinars, social networking, remote medical treatments, government services, VoIP, and net browsing. Yet, a limitation to these online services is the primary infrastructure of the public Internet, which permits an attacker to temper, interrupt, and spy on the transmitted messages amongst two trusted entities. Hence, it has become the most significant factor to ensure the transmitted messages' security, including the user's privacy. Further, the technology of advanced cloud computing has provided economical and flexible service to its users, making massive amounts of confidential multimedia data being outsourced on the cloud, leading to risks and privacy concerns associated with this data. The preservation of privacy has emerged to be one of the hot topics during a few years in the domains of cloud computing. Provided with the facts that, once the data of some user gets compromised, there could be several negative results. As a result, the construction of technologies linked to the preservation of privacy has emerged as a fundamental concern in the cloud computing domain.

Cloud computing technology provides cost-saving and flexibility of services for users. With the explosion of multimedia data, more and more data owners would outsource their personal multimedia data on the cloud. In the meantime, some computationally expensive tasks are also undertaken by cloud servers. However, the outsourced multimedia data and its applications may reveal the data owner's private information because the data owners lose control of their data. Recently, this thought has aroused new research interest on privacy-preserving reversible data hiding over outsourced multimedia data. Anonymous Authentication Scheme will be proposed in this chapter as the most relatable, applicable,

Related Content

Tissue Image Classification Using Multi-Fractal Spectra

Ramakrishnan Mukundanand Anna Hemsley (2010). *International Journal of Multimedia Data Engineering and Management (pp. 62-75).*

www.irma-international.org/article/tissue-image-classification-using-multi/43748

"The More I Write…The More My Mind Evolves Into Something Outstanding": Composing Identities with Social Media Tools

Mary Beth Hines, Jennifer M. Conner-Zachockiand Becky Rupert (2018). *Digital Multimedia: Concepts, Methodologies, Tools, and Applications (pp. 333-347).*

www.irma-international.org/chapter/the-more-i-writethe-more-my-mind-evolves-into-something-outstanding/189481

A Real-Time 3D Visualization Framework for Multimedia Data Management, Simulation, and Prediction: Case Study in Geospatial-Temporal Biomedical Disease Surveillance Networks

Nathaniel Rossol, Irene Cheng, Iqbal Jamal, John Berezowskiand Anup Basu (2011). *International Journal of Multimedia Data Engineering and Management (pp. 1-18).*

www.irma-international.org/article/real-time-visualization-framework-multimedia/54459

Content-Based Multimedia Retrieval

Chia-Hung Weiand Chang-Tsun Li (2005). *Encyclopedia of Multimedia Technology and Networking (pp. 116-122).*

www.irma-international.org/chapter/content-based-multimedia-retrieval/17236

Using a Commodity Hardware Video Encoder for Interactive Applications

Håkon Kvale Stensland, Martin Alexander Wilhelmsen, Vamsidhar Reddy Gaddam, Asgeir Mortensen, Ragnar Langseth, Carsten Griwodzand Pål Halvorsen (2015). *International Journal of Multimedia Data Engineering and Management (pp. 17-31).*

www.irma-international.org/article/using-a-commodity-hardware-video-encoder-for-interactive-applications/132685