# Multimedia Information System Security

## Dr WASAN MEHDI

# Overview

- Objectives
- Introduction
- Architecture of Multimedia
- Security Issues
- Latest Technical solutions
- Conclusion
- Future work

# Objectives

1. To give thorough review to MISS, and to introduces a general architecture of multimedia information system.
2. Investigates some security issues in MIS, and reviews the latest security solutions
3. To review the latest technical solutions
4. Illustrate other security issues

# Introduction

With the fast advance development of the Internet and Multimedia techniques, the Security protection of multimedia content, service interaction and user privacy, etc. has become increasingly important. For example, the content related to commercial secret needs to be protected against unauthorized users, payment interactions between the user and the retailer is sensitive to the third party, and the user profiles are private and should not be published.

One of many advantages it has is enabling multimedia data's, generation, editing, sharing storage, etc. Despite the obvious progress, these developments carry with them a number of risks such as copyright violation, prohibited usage and distribution of digital media, etc. Therefore, security, scalability and manageability amongst others become issues of serious concern, as current solutions do not satisfy anymore the growing demands of Multimedia communications.

The scope and target of this work is the focus on reviewing Multimedia Information and System Security MISS, and to provide the latest advance security solutions such as Digital confidentiality protection, Digital ownership Rights Management (DRM), forgery detection, protection, traitor tracing, secure multimedia distribution based on watermarking, copy detection, etc..

# 1. Architecture review of MIS

The general architecture of MIS is depicted in figure 1 and studied by *[Rahman 2007]*.
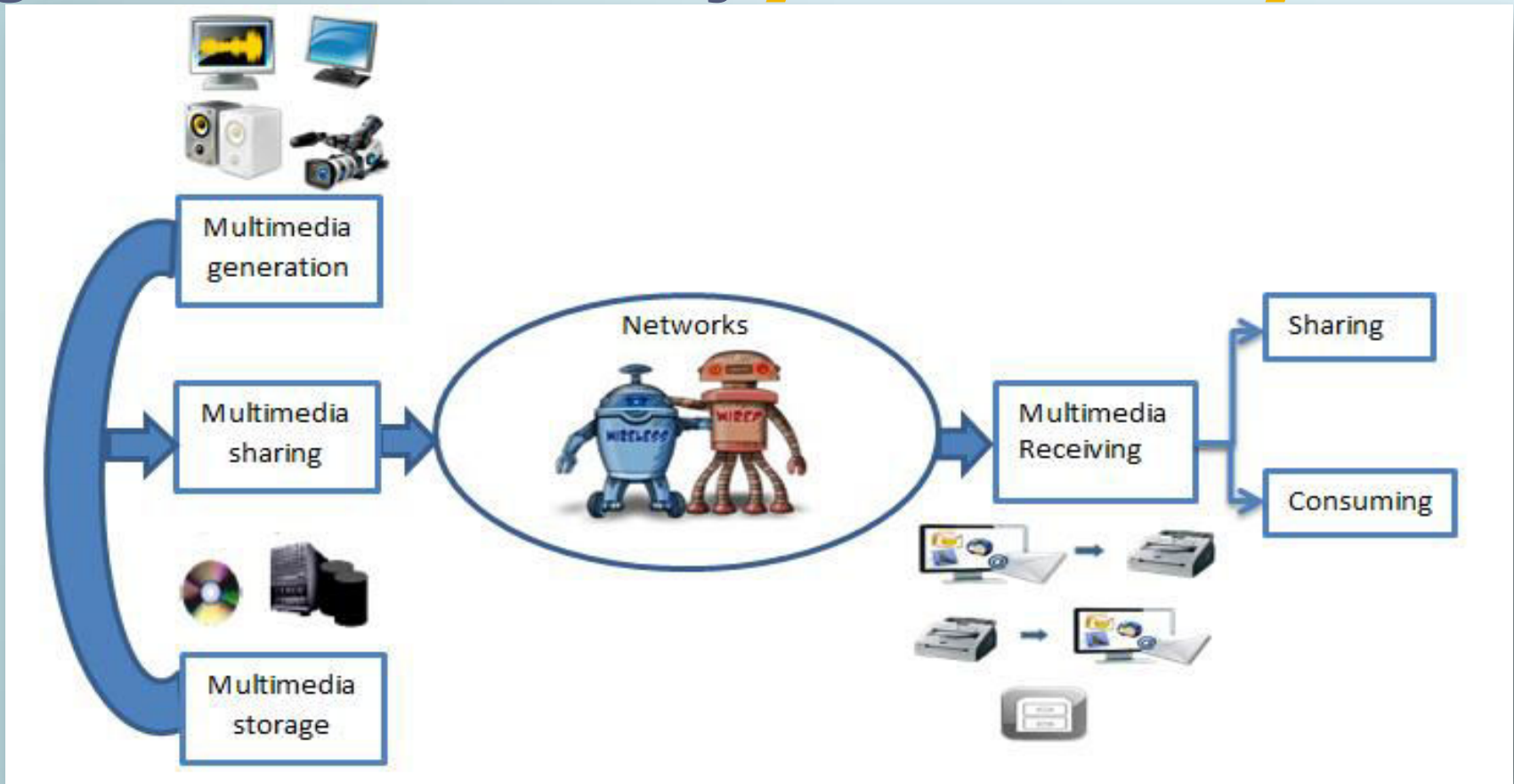


Figure 1 architecture of MIS

***Multimedia content generation:*** **It denotes the process to generate multimedia content produces (film, music, flash, web, etc.). Cameras, Digital Video, audio recorder, etc. are generally used in this process. The multimedia content is usually requires a professional producers, while, for normal users there are no limitation to producers.** *[Rahman 2001].*

***Multimedia storage & management*** **the content is often stored and backed up before being transmitted. For example, the film is recorded, the music is burned into a compact Disc, and the videos or web data are buffered in the computer servers in order to make the data access more convenient, therefore, the contents and their index information are ordered and stored in the database, while some search or data mining techniques can be used. As a consequence, the need for an efficient management and the save to the storage cost, multimedia content is often compressed.**

***Multimedia distribution*** **transmits the content from one user to others. There are two kinds of multimedia content to be transmitted, 1.** *Real-time content* **and 2.** *Stored content.*

**1. denotes the generated content without delayed storage, e.g. live TV or telephone call.**

**2. denotes the content stored in the database, e.g. video clips, music, web data.**

# 2. Security issues in MIS

Security issues has been generated from the transmitted information's sensitivities, studied by [Thuraisingham 2007], which may be directed to military or personal privacy access to authorised users only. With respect to the complexity of the information system, there are various issues / threats these are: **Privacy, Intrusion, Piracy, Forgery,**

- **Privacy:** Privacy is about respecting the desires of individuals and is not just about what people expect but about what their desire too. In MIS some personal information is private e.g. login info, however in social media users can produce or post some multimedia content that is shared with other users. The user generated contents may be also private.

- **Forgery:** The crime of creating a false document, altering a document, or writing a false signature for the illegal benefit of the person making the forgery. This includes improperly filling in a blank document, like an automobile purchase contract, over a buyer's signature, with the terms different from those agreed.

**Intrusion:** is the act of gaining unauthorized access to a system. One of its goals is to remain undetected for as long as possible so that they can continue with their malicious activity undisturbed. These attempts may take the form of malware, crackers etc. in order to attacks unsafe network, server and host taking advantages of the weakness of multimedia service systems to disable them in addition to the opportunity to tamper with software/hardware data.

**Piracy:** The act of illegal copying, distribution, or use of software. It is such a profitable "business" that it has caught the attention of organized crime groups in a number of countries.

Types of software piracy include:

‣ **Soft-lifting:** Borrowing and installing a copy of a software application from a colleague.

‣ **Client-server overuse:** Installing more copies of the software than you have licenses for.

‣ **Hard-disk loading:** Installing and selling unauthorized copies of software on refurbished or new computers.

‣ **Counterfeiting:** Duplicating and selling copyrighted programs.

‣ **Online piracy:** Typically involves downloading illegal software from peer-to-peer network, Internet auction or blog.

# 3. Latest technical solutions

To resolve the security issues in multimedia information systems, some solutions can address media source identification, such as ownership protection, copy detection, confidentiality protection, forgery detection etc. The particular type techniques include Digital Rights Management *(DRM),* multimedia encryption, digital watermarking, digital fingerprinting, multimedia forensics, privacy, data mining, secure user interface, intrusion detection, etc.

# 4. Other security issues

There are many other solutions focus on special applications in Multimedia information system security. Some other new solutions are expected to merge. We can describe them as follow:

## Intelligent surveillance

Cameras and collected data volumes are increasingly distributed as surveillance, Maybank 2004. it processes the multimedia data automatically to extract usable information. The intelligent processing techniques include object such as tracking, activity analysis, crime detection etc. and other techniques such as video machine learning and so on.

## Security of content sharing in social media

The content sharing in social media attracts user's activities, some of these media networks environment such like Blog, flickers, where users can upload or post multimedia content as they wish.

Although it has noted that, more undesirable contents arise in these Medias, e.g., piracy, terror. To detect or prevent these contents' distribution is a new area and some content analysis and classification techniques need to be used together with existing security solutions.

## *Security in network*

Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more and more people joined to a network, an increasing number of people need to understand the basics of security in a networked world, the risks and how to deal with them. These challenges includes not only the exchange of network protocols, the bit-rate adaptation of multimedia content and the compliance of user terminals but also the security architecture covering all the involved networks.

## *Trusted Computing*

is recently proposed to construct a fully trusted system. It aims to solve the security issues caused by software-only means, which enforces the trusted behaviour by loading the hardware with a unique ID and key.

# 5. Conclusion

We have introduced a general view of multimedia information system architecture, addressed the important security issues and some typical technical solutions has also been reviewed. We believe that this paper is expected to provide valuable information to users working in multimedia information system security

Therefore, in this presentation we have discussed some important security issues such as: intrusion, forgery, piracy and privacy, and reviewed only some typical solutions such as Digital Rights Management (DRM),confidentiality protection, ownership protection, traitor tracing, secure multimedia distribution based on watermarking, forgery detection, copy detection,

# 5. Conclusion

privacy-preserving data mining, secure user interface, and intrusion detection and prevention. As the demands for multimedia information systems arise, new security issues will be generated. We are inclined to the fact that the research will continue to resolve major security issues by proposing novel approaches. For this reason our aim in the near future to update our work by adding the new issues and provide solutions.

# Future Work

There has been a tremendous improvement in multimedia processing techniques in the past decade. With this continuous advancement, the problem of MISS has become vital topic in both private sector and government application due to criminal activities and malicious intent. In order to protect and prevent this kind of activities we have thought of controlling our systems involve by filtering, categorising, and limiting words and links, by displaying an alert message to the user. Also full control on all the computers and peripheral on site. Making the system /computers as *trusted computers*. A hard copy of machine and user identification can be displayed to tackle any problem.

# THANK YOU VERY MUCH FOR LISTENING

**wasan.mehdi@beds.ac.uk**
**Or**
**mehdi_wasan@hotmail.com**