

MOP: A Privacy Preserving Model for Multimedia Objects

Ramzi A. Haraty and Mohammad A. Taha

Department of Computer Science and Mathematics

Lebanese American University

Email: {rharaty, mohammad.taha@lau.edu.lb}

Bechara Al Bouna

Ticket Labs

Antonine University

Baabda, Lebanon

Email: bechara.albouna@upa.edu.lb

ABSTRACT

Recently, multimedia and internet technologies have been in rapid development. Multimedia objects, such as images, video, audio tracks and multimedia documents, have been widely used and are in remarkable growth. Almost everyone on social network publishes or has some multimedia objects stored somewhere. Although multimedia objects are of different types, they can be treated as one entity when it comes to privacy which is our concern in this paper. Many researchers tried to apply some security on multimedia objects. In this work we aim to provide a model to protect multimedia objects from being accessed or altered by unwanted personnel.

Categories and Subject Descriptors

K.4 COMPUTERS AND SOCIETY, K.4.1 Public Policy Issues

General Terms

Security

Keywords

Multimedia objects, Security, Privacy, and Social Networks.

1. INTRODUCTION

In order to publish a multimedia object freely on any social network without the fear of this object being used by an unwanted user intending to harm its owner, an imperative step to be considered is privacy. The multimedia object owner should be in control and aware of the users that can view or alter some of the entities of his/her owned items.

The owner of the multimedia object should be in full control of the objects visible to others in his/her profile. Most of the social networking services provide some security levels in order for the owner of the multimedia objects to have privacy control by choosing the appropriate level of security depending on the importance of the objects or on the types of users that will view the profile. In this paper, we highlight several multimedia privacy models, which are of great help to the understanding of the privacy of multimedia object models. We also introduce a model, which is based on a formal representation of a system's entities and the relationship between these entities. Using Alloy Language and Analyzer, we can have a consistent system that contains our privacy policy requirements.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

MEDES'14, September 15-17, 2014, Buraidah Al Qassim, Saudi Arabia.

Copyright © 2014 ACM 978-1-4503-2767-1/10/10...\$10.00.

<http://dx.doi.org/10.1145/2668260.2668280>

The development of multimedia object privacy model in this report is based on Alloy. Alloy is a small language that describes structural properties [1]. Alloy supports a graphical representation or textual declaration of the basic structures of the models. The language is based on logical formulas that can check for consequences and consistencies. This is achieved by analyzing the model, understanding the constraints, and authenticating these constraints by checking the consistency according to some defined rules. Alloy can be used to model and analyze a set of models, including privacy and integrity models, security models, and other types that can include analysis of UML, mobile internet protocols, and architectural frameworks. After analyzing such models, Alloy can check their consistency and inconsistency. The advantage of Alloy language and analyzer can be described as the ability to analyze systems that are dynamically changed. Another advantage is allowing the user to check for the consistency of the model before implementing it.

Lately, many researchers studied the privacy of multimedia objects. In this paper, our created model will be based on a previous research by [2-3]. Their work introduced a data model that can describe the multimedia objects that are published on social network. In our work, we show the relationship of multimedia objects' entities and the group of users collected from the above sources. Using Alloy Language and Analyzer tool, we will be able to show that privacy and integrity of our model are consistent when users and entities are combined together.

The remainder of the paper is organized as follows. Section 2 highlights related works. Section 3 introduces the formal privacy policy model. Section 4 discussed the multimedia object privacy model, and section 5 concludes the paper.

2. RELATED WORK

Joshi et al. proposed a multimedia document model that allows a secure access to multimedia document database [4]. The model uses multilevel security [5]. The proposed model provides an application-level, user-defined classification structures of multimedia documents. Joshi specified the restriction between inter-domains when subject/objects are administered by different level of policies in a multi-domain environment. This will create complex documents that belong to different domains and contain multilevel objects. This will result in providing a single document that contains different sets of information for different users. Joshi also proposed the temporal constraint system that generalizes both deterministic and nondeterministic temporal relations knowing that a priori knowledge about interval durations and/or interval end do not exist.

Kodali et al. presented an authorization model for multimedia digital libraries [6]. Different approaches were presented in this

paper. The original security need of the data object is guaranteed; this is basically the goal of their approach. Moreover, a transparent access to data object is allowed without worrying about the applied security model. A generalized security framework was developed to represent Discretionary Access Control, Mandatory Access Control and Role Based Access Control. The representation of access control is done using SMIL, synchronized multimedia integration language that is an extension to XML. SMIL is used to authorize multimedia documents, to define protection objects and to represent access control and QoS requirements. Hangzai et al. proposed a novel approach for privacy-preserving video sharing [7]. A new framework is proposed to protect the video content privacy. The framework is able to address the security challenges that arise throughout video sharing. The proposed algorithm tackles three main security problems: owner-adaptive video privacy modeling, video content privacy protection and interference control. Based on the three observations, the proposed algorithm assures the privacy of video content being shared. In addition, the algorithm improves the classifier's accuracy and limiting the privacy breaches by determining the optimal size of the blurred samples for classifier validation. Their experiments were carried out on a specific domain, and the results showed effectiveness of their technique.

Lian et al. [8] introduced Digital Rights Management (DRM) to protect the multimedia contents. The scope of DRM takes into consideration the data to be protected such as image, video, audio, text, etc. DRM was proposed as a solution to some important security issues related to multimedia objects such as intrusion, the act of unwanted attempts at accessing or manipulating multimedia contents, piracy which can be classified into two types: unauthorized access and unauthorized distribution of multimedia contents, and privacy - for example - in social networks where users can post some multimedia content that could be either shared or private. Ridzon and Levicky [9] tackled multimedia security and multimedia content protection. They elaborated the requirements of multimedia security and protection of ownership. The three main groups of multimedia security are as follows: the ownership rights protection, the distribution of illegal copies, and finally the unauthorized access to multimedia content. The multimedia content protection consists of two phases: the first is to protect multimedia during transmission. This could be established through cryptographic methods which secure the multimedia content by encryption such as DRM. The other phase is to protect multimedia after transmission. This could be established through watermarking techniques, where the content of multimedia is changed slightly and visually undetectable.

Al Bouna et al. worked on enforcing role based access control model with multimedia signature [10]. They tackled access control models specifically the impact of RBAC integrated with multimedia based information. The model is able to handle the revealing of information and providing enforced access decisions due to the relation between multimedia signatures to roles and permissions. A multimedia signature can be linked either to a role to define role description using multimedia objects, or to a permission to represent the environment (people nearby, location, etc.). Whenever a user wants to activate a role belonging to multimedia-signature, validation should be done ahead of time in order to receive the linked permissions. Also, when a user wants to perform a specified operation that is an assigned permission, the multimedia signature related to permission should be validated. Al Bouna et al. [11] also prototype a toolkit called

image protector is used to specify authorization that is done using the SWRL specification module. Authorization is to define some security rules on multimedia objects. Authentication is based on username and password. The BackOffice and FrontOffice modules constitute the two main modules of image protector. A BackOffice module is used to specify security rules using an authorization manager; also, the BackOffice is used to manage multimedia objects. While the FrontOffice module supports querying multimedia objects, actions and protection mechanisms are established to display the filtered content in three different formats: pixelize, blur, and spiral.

Saad et al. proposed a model to detect possible data associations that is a major element making confidential multimedia objects at risk [12]. The authors proposed a technique to detect potential implications related to data association where an unauthorized user is able to disclose confidential multimedia objects that are protected by access control mechanisms as with [11]. Saad's technique is based on a multimedia co-occurrence matrix and a tree augmented naïve Bayesian network with the capability to contain authorization manager that could detect threats to data associations. In order to detect a data association, Saad built a tree augmented with several key attributes, and based on those attributes, data associations are detected.

Ben Dhia et al. described access control mechanisms that can determine whether access is granted or denied for the multimedia object being accessed based on constraints and access rules [13].

Zhuo et al. discusses privacy issues concerning the user's personal information retrieval that could harm its owner [14]. The user's information is gathered by feedback collected from different users. Zhuo and his colleagues proposed a technique to provide better personalized retrieval to make the user satisfied while preserving his/her privacy. The method is called controllable privacy that is based on a simple tree structure of ODP [15] and the user's information. In order to meet the different levels of privacy requirements, the authors constructed a hierarchical structure profile. Users can choose between the three levels of privacy, which are no privacy, low privacy and high privacy for better protection of their privacy in image retrieval.

3. FORMAL PRIVACY POLICY MODEL

In this section, we briefly overview the Alloy language and demonstrate how a model can be checked for consistency.

3.1 The Alloy Language

To formalize our privacy model, we use the Alloy language and its analyzer. Alloy is a lightweight modeling formalism using a first order predicate logic over the domain of relations. These relations are similar to relational algebra and calculus.

3.2 Alloy Language Features

The following features present a subset of the full Alloy language that we used in formalizing our privacy model. An Alloy model consists of one or more files, each containing a single module. A module consists of a header identifying the module, some imports and some paragraphs:

```
module::Dheader-import*paragraph*
```

A model can be contained entirely within one module. The paragraphs of module are signatures, facts, functions, predicates, assertions, run commands, and check commands.

Alloy uses the following multiplicity keywords: *lone*: zero or one; *one*: exactly one; *some*: one or more; *set*: zero or more. These keywords are used as quantifiers in quantified formulas, quantified expressions, in set declarations, in relation declarations, and in signature declarations. A signature represents a set of atoms and is declared using the “sig” keyword—such as *sig A {}* to define a signature named *A*. The types of signatures are: *subset*, *top-level*, and *abstract*, and a signature with a *multiplicity* keyword:

- A top-level signature represents mutually disjoint sets that does not extend another signature: *sig A {}*
- A subset signature represents a set of elements that is a subset of the union of its parents: *one sig B extends A {}*
- An abstract signature represents only the elements that belong to one of the signatures that extend it: *abstract sig A {}*
- A signature with multiplicity keyword constrains the signature’s set to have the number of elements specified with the keyword.

Facts, functions, and predicates are packages of constraints. A fact is a constraint that always holds. A predicate is a template for a constraint that can be instantiated in different contexts. A function is a template for an expression, and an assertion is a constraint that is intended to follow from the facts of a model. Examples of facts, predicates, and assertions are:

```
fact {no iden & parent}
pred access(state: State, next: state, u: User, r: Resource)
{next.accessed D state.accessed C u -> r}
assert example1 {
A.sens D SecretNT
B.sens D SecretT}
```

Run and check commands are used to instruct the Alloy analyzer to perform various analyses. A run command causes the analyzer to search for an instance that shows the consistency of a function or a predicate, whereas a check command causes it to search for a counterexample showing that an assertion does not hold:

```
check example
run MOPModel
```

4. THE MULTIMEDIA OBJECT PRIVACY (MOP) MODEL

Depending on the multimedia object being published, a user should pay a great deal of attention to securing this object. Many strategies have been studied and implemented [16-18]. In our model, we use the privacy concerns which include the privacy levels that Aimeur et al. proposed [2]. In addition, we will describe the most important entities that constitute a multimedia object based on a study done on some essential social networking sites. The entities are keyword, URL, Event, Location, Articles, Tweets, and Username; these entities will be described in details later in this section.

The user privacy concern is classified into three main divisions: the first is the security issues which constitute an important factor that is to protect the multimedia object from unauthorized users that can harm the user’s data and information. The second is reputation; when unwanted users are allowed to view your profile,

which will sometimes, if used improperly, endanger the reputation of entrepreneurs. This could happen by publishing a boring post, disrespecting others, failing to promote others, and finally being tagged on uncertain multimedia objects. The third is profiling which means allowing unauthorized users to access your profile which will sometimes, if used improperly, result in building a fake profile using user’s information and data without his/her being aware of it.

The multimedia object is divided into seven main attributes:

- Keyword: the set of words that describe the multimedia object
- URL: the resolution location of the multimedia object
- Event: Set of words that describe the event of the multimedia object item
- Location: Set of words that describe the actual location of the event being held
- Articles: Set of published articles on the event being held
- Tweets: Set of comments a user can post about the multimedia object
- Username: The actual location that contains the owner of the multimedia object.

The main purpose of these attributes is to give the owner the flexibility to enforce restrictions on each attribute, and not only on a multimedia object as a whole.

After partitioning the multimedia object attributes, and identifying who can access the attributes, a user is classified depending on the relationship between the owner of the multimedia object and different types of users. The types of users are classified as follows:

- Owner: The owner of the multimedia object being published
- Related: A person appearing in the multimedia object being published
- Friend: A person that is a friend of the Owner or Related person
- Cyber-stalker: An anonymous person that could be destructive if exposed to multimedia objects being published.

The MOP model that will combine the attributes along with the users will deal with the privacy that the owner could enforce on his/her data being published. The privacy levels are divided into four types: Low privacy, Soft privacy, Hard privacy and Full privacy. The least restrictive is the Low privacy level and the most restrictive is the Full privacy. Each of these levels has its own rules on each group of users. The rules are made in order to read, insert and delete on the attributes of multimedia object:

- Low Privacy Rules: Owner can read all attributes and can insert/delete Articles and Tweets, Related can read all attributes and can insert/delete Articles and Tweets, Friends can read all attributes and can insert Articles and Tweets but cannot delete Articles or Tweets, and Cyber-stalker can read all attributes and can insert Articles and Tweets but cannot delete Articles or Tweets.
- Soft Privacy Rules: Owner can read all attributes and can insert/delete Articles and Tweets, Related can read all attributes and can insert/delete Tweets insert Articles but cannot delete Articles, Friends can read all attributes; can insert Articles and Tweets but cannot delete Articles or Tweets, and Cyber-stalker cannot read Keyword, Location, Event; can read URL, Articles, Tweets and Username but cannot insert or delete Articles or Tweets.

- Hard Privacy Rules: Owner can read all attributes and can insert/delete Articles and Tweets, Related can read all attributes, can insert Articles and Tweets but cannot delete Articles or Tweets, Friend cannot read Keyword, Location, Event, can read URL, Articles, Tweets and Username, can insert Tweets but cannot insert or delete Articles, and cannot delete Tweets, and Cyber-stalker cannot read Keyword, Location, Event, Articles, can only read URL, Tweets and Username, cannot insert or delete Articles or Tweets.
- Full Privacy Rules: Owner can read all attributes and can insert/delete Articles and Tweets; Related can read all attributes except for the Location, cannot insert or delete Articles or Tweets, Friend cannot read Keyword, Location, Event can read URL, Articles, Tweets and Username, cannot insert or delete Articles or Tweets, and Cyber-stalker cannot read any attribute, cannot insert or delete Articles or Tweets.

Table 1 summarizes the privacy settings, privacy levels, and users as follows:

Table 1. Multimedia object privacy model rules.

Privacy settings	Entity	Multimedia Object						
		Keyword	URL	Location	Event	Articles	Tweets	Username
Low	Yes	Yes	Yes	Yes	R/I/D	R/I/D	Yes	Owner
	Yes	Yes	Yes	Yes	R/I/D	R/I/D	Yes	Related
	Yes	Yes	Yes	Yes	R/I/ND	R/I/ND	Yes	Friend
	Yes	Yes	Yes	Yes	R/I/ND	R/I/ND	Yes	Cyber-stalker
Soft	Yes	Yes	Yes	Yes	R/I/D	R/I/D	Yes	Owner
	Yes	Yes	Yes	Yes	R/I/ND	R/I/ND	Yes	Related
	Yes	Yes	Yes	Yes	R/I/ND	R/I/ND	Yes	Friend
Hard	No	Yes	No	No	R/NI/ND	R/NI/ND	Yes	Cyber-stalker
	Yes	Yes	Yes	Yes	R/I/D	R/I/D	Yes	Owner
	Yes	Yes	Yes	Yes	R/I/ND	R/I/ND	Yes	Related
Full	No	Yes	No	No	R/NI/ND	R/NI/ND	Yes	Friend
	No	Yes	No	No	R/NI/ND	R/NI/ND	Yes	Friend
	No	No	No	No	NR/NI/ND	NR/NI/ND	No	Cyber-stalker
	No	No	No	No	NR/NI/ND	NR/NI/ND	No	Cyber-stalker

As shown in Table 1, the Multimedia Object Privacy Model is split into four groups: Low Privacy, Soft Privacy, Hard Privacy and Full Privacy. In Low Privacy Level (LowP), Low privacy users (Lusers) are divided into four categories: Owner (LO), Related (LR), Friend (LF) and Cyber-stalker (LC); (LO) has the right to read all the seven attributes of multimedia object. The attributes include Keyword (LowPKeyMO), URL (LowPURLMO), Location (LowPLocMO), Event (LowPEveMO), Articles (LowPArtMO), Tweets (LowPTwtMO), and Username (LowPUsernameMO) but LF and LC cannot delete LowPTwtMO and LowPArtMO. In Soft Privacy Level (SoftP), Soft privacy users (Susers) from the three categories SO, SR, and SF have the right to read all multimedia object attributes; SO can insert/delete SoftPTwtMO and SoftPArtMO as for SC cannot read SoftPKeyMO, SoftPLocMO and SoftPEveMO cannot insert/delete SoftPTwtMO and SoftPArtMO. SR and SF can insert SoftPArtMO and SoftPTwtMO. SR and SF cannot delete SoftPArtMO. SoftPTwtMO cannot be deleted by SF but SR can delete SoftPTwtMO. In Hard Privacy Level (HardP), Hard privacy users (Husers) from all categories HO, HR, HF and HC can read some attributes from HardPKeyMO,HardPURLMO, HardPLocMO, HardPEveMO, HardPArtMO, HardPTwtMO and HardPUsernameMO; HF and HC cannot read HardPKeyMO, HardPLocMO, and HardPEveMO. HR, HF and HC cannot delete HardPArtMO, and HardPTwtMO. HC cannot read/insert

HardPArtMO. HC cannot insert HardPTwtMO. Finally HF cannot insert HardPArtMO. In Full Privacy Level (FullP), Full privacy users (Fusers) from all categories FO, FR, FF, and FC can read some attributes of FullPKeyMO, FullPURLMO, FullPLocMO, FullPEveMO, FullPArtMO, FullPTwtMO, and FullPUsernameMO. FC cannot read/insert/delete all of the above attributes. FR cannot read FullPLocMO. FF cannot read FullPKeyMO, FullPLocMO, and FullPEveMO. FR and FF cannot insert/delete FullPArtMO, and FullPTwtMO. Table 2 lists the privacy data set levels.

The Allow implementation, divided into sections, is as follows:

- Section 1 declares the system entities of the Privacy Data Sets. It also explains the Privacy Levels as part of the Privacy Data Set.

```

one sig LowPKeyMO,LowPURLMO,LowPLocMO,LowPEveMO,LowPUsernameMO extends LowP
{readyby: some Lusers}
one sig LowPArtMO,LowPTwtMO extends LowP
{readyby: some Lusers,insertby: some Lusers, deleteby: some Lusers}
one sig SoftPKeyMO,SoftPURLMO,SoftPLocMO,SoftPEveMO,SoftPUsernameMO extends SoftP
{readyby: some Susers}
one sig SoftPArtMO,SoftPTwtMO extends SoftP
{readyby: some Susers,insertby: some Susers, deleteby: some Susers}
one sig HardPKeyMO,HardPURLMO,HardPLocMO,HardPEveMO,HardPUsernameMO extends HardP
{readyby: some Husers}
one sig HardPArtMO,HardPTwtMO extends HardP
{readyby: some Husers,insertby: some Husers, deleteby: some Husers}
one sig FullPKeyMO,FullPURLMO,FullPLocMO,FullPEveMO,FullPUsernameMO extends FullP
{readyby: some Fusers}
one sig FullPArtMO,FullPTwtMO extends FullP
{readyby: some Fusers,insertby: some Fusers, deleteby: some Fusers}

```

Section 1 MOP declarations of privacy data sets in each level.

- Section 2 explains the users' groups. In our model we have four types: Lusers, Susers, Husers and Fusers.

```

abstract sig Lusers{} //Low Privacay Users
abstract sig Susers{} //Soft Privacay Users
abstract sig Husers{} //Hard Privacay Users
abstract sig Fusers{} //Full Privacay Users

```

Section 2 MOP system entities declaration.

- Section 3 explains the privacy data sets in each level as part of the privacy levels. Table 2 provides explanation of each level.

```

abstract sig PrivacyDS {} // Privacy Data Set
abstract sig LowP extends PrivacyDS{}
abstract sig SoftP extends PrivacyDS{}
abstract sig HardP extends PrivacyDS{}
abstract sig FullP extends PrivacyDS{}

```

Section 3 MOP user group data set.

Table 2. Privacy data set levels.

Privacy Data Set Levels	Description
PrivacyDS	Privacy Data Set
LowP	Low Privacy Data Set
SoftP	Soft Privacy Data Set
HardP	Hard Privacy Data Set
FullP	Full Privacy Data Set

- Section 4 explains the declaration of the users in each level of the privacy data set. This is explained in Table 43.

Declaration of Low Privacy Users	Declaration of Soft Privacy Users
<pre>//Declaration of Low Privacy Users one sig LO extends Users{} one sig LR extends Users{} one sig LF extends Users{} one sig LC extends Users{}</pre>	<pre>//Declaration of Soft Privacy Users one sig SO extends Susers{} one sig SR extends Susers{} one sig SF extends Susers{} one sig SC extends Susers{}</pre>
Declaration of Hard Privacy Users	Declaration of Hard Privacy Users
<pre>//Declaration of Hard Privacy Users one sig HO extends Husers{} one sig HR extends Husers{} one sig HF extends Husers{} one sig HC extends Husers{}</pre>	<pre>//Declaration of Full Privacy Users one sig FO extends Fusers{} one sig FR extends Fusers{} one sig FF extends Fusers{} one sig FC extends Fusers{}</pre>

Section 4 MOP declarations of users on each level.

Table 3. Privacy data set according to each level.

Low privacy data set	Description	Soft privacy data set	Description
LowPKeyMO	Low Privacy on Keyword	SoftPKeyMO	Soft Privacy on Keyword
LowPURLMO	Low Privacy on URL	SoftPURLMO	Soft Privacy on URL
LowPLocMO	Low Privacy on Location	SoftPLocMO	Soft Privacy on Location
LowPEveMO	Low Privacy on Event	SoftPEveMO	Soft Privacy on Event
LowPArtMO	Low Privacy on Articles	SoftPArtMO	Soft Privacy on Articles
LowPTwtMO	Low Privacy on Tweets	SoftPTwtMO	Soft Privacy on Tweets
LowPUsernameMO	Low Privacy on Username	SoftPUsernameMO	Soft Privacy on Username
Hard privacy data set	Description	Full privacy data set	Description
HardPKeyMO	Hard Privacy on Keyword	FullPKeyMO	Full Privacy on Keyword
HardPURLMO	Hard Privacy on URL	FullPURLMO	Full Privacy on URL
HardPLocMO	Hard Privacy on Location	FullPLocMO	Full Privacy on Location
HardPEveMO	Hard Privacy on Event	FullPEveMO	Full Privacy on Event
HardPArtMO	Hard Privacy on Articles	FullPArtMO	Full Privacy on Articles
HardPTwtMO	Hard Privacy on Tweets	FullPTwtMO	Full Privacy on Tweets
HardPUsernameMO	Hard Privacy on Username	FullPUsernameMO	Full Privacy on Username

- In Section 5, the instances of users that belong to the different privacy data set levels are declared. LR1 and LR2 are two users that belong to the category of Related in Low privacy level. Similarly, SC1 and SC2 belong to the category of Cyber-stalkers of the Soft Privacy Level. The rest are instances of users at different privacy levels.

Declaration of No Privacy Users instances	Declaration of Soft Privacy Users instances
<pre>//Declaration of Groups of Users Instances one sig LR1,LR2 in LR{} one sig LF1,LF2 in LF{} one sig LC1 in LC{} one sig LO1 in LO{}</pre>	<pre>one sig SR1,SR2 in SR{} one sig SF1 in SF{} one sig SC1,SC2 in SC{} one sig SO1 in SO{}</pre>
Declaration of Hard Privacy Users instances	Declaration of Full Privacy Users instances
<pre>one sig HR1 in HR{} one sig HF1 in HF{} one sig HC1 in HC{} one sig HO1 in HO{}</pre>	<pre>one sig FR1 in FR{} one sig FF1 in FF{} one sig FC1 in FC{} one sig FO1 in FO{}</pre>

Section 5 MOP declarations of users' instances on each level.

- Section 6 shows the constraints for "Low Privacy" level (LowP). It shows that a Friend and Cyber-stalker cannot delete LowPArtMO and LowPTwtMO.

```
fact{
//Deleteby constraints on Low privacy Model
LowPArtMO.deleteby!=LF
LowPTwtMO.deleteby!=LF
LowPArtMO.deleteby!=LC
LowPTwtMO.deleteby!=LC
}
```

Section 6 Constraints on Low Privacy.

- Section 7 shows the constraints for "Hard Privacy" level (HardP). It shows that a Cyber-stalker and a Friend cannot read HardPKeyMO, HardPLocMO, and HardPEveMO and a Cyber-stalker cannot read/insert/delete HardPArtMO and he

cannot insert/delete HardPTwtMO. A Friend and a Related cannot delete HardPTwtMO and HardPArtMO.

```
fact{
//Readby Constraints on Hard Privacy data set
HardPKeyMO.readby!=HF
HardPKeyMO.readby!=HC
HardPLocMO.readby!=HF
HardPLocMO.readby!=HC
HardPEveMO.readby!=HF
HardPEveMO.readby!=HC
HardPArtMO.readby!=HC
//Insertby constraints on Hard Privacy data set
HardPArtMO.insertby!=HC
HardPArtMO.insertby!=HF
HardPTwtMO.insertby!=HC
//Deleteby constraints on Hard Privacy set
HardPArtMO.deleteby!=HF
HardPArtMO.deleteby!=HR
HardPTwtMO.deleteby!=HF
HardPTwtMO.deleteby!=HR
HardPArtMO.deleteby!=HC
HardPTwtMO.deleteby!=HC
}
```

Section 7 Constraints on Hard Privacy.

- Section 8 shows the constraints at the "Full Privacy" level (FullP). It shows that a Cyber-stalker cannot read FullPKeyMO, FullPURLMO, FullPLocMO, FullPEveMO, FullPArtMO, FullPTwtMO, and FullPUsernameMO. A Cyber-stalker cannot insert/delete FullPArtMO, and FullPTwtMO. A Related cannot read FullPLocMO. A Friend cannot read FullPKeyMO, FullPLocMO, and FullPEveMO. A Related and a Friend cannot insert/delete FullPArtMO, and FullPTwtMO.

```
fact{
//Readby Constraints on Full Privacy data set
FullPKeyMO.readby!=FF
FullPKeyMO.readby!=FC
FullPURLMO.readby!=FC
FullPLocMO.readby!=FR
FullPLocMO.readby!=FF
FullPLocMO.readby!=FC
FullPEveMO.readby!=FF
FullPEveMO.readby!=FC
FullPArtMO.readby!=FC
FullPTwtMO.readby!=FC
//Insertby constraints on Full Privacy data set
FullPArtMO.insertby!=FC
FullPArtMO.insertby!=FF
FullPArtMO.insertby!=FR
FullPTwtMO.insertby!=FC
FullPArtMO.insertby!=FF
FullPTwtMO.insertby!=FR
//Deleteby constraints on Full Privacy set
FullPArtMO.deleteby!=FF
FullPArtMO.deleteby!=FR
FullPTwtMO.deleteby!=FF
FullPTwtMO.deleteby!=FR
FullPArtMO.deleteby!=FC
FullPTwtMO.deleteby!=FC
}
```

Section 8 Constrains on Full Privacy.

- Section 9 shows the constraints for "Soft Privacy" level (SoftP). It shows that Cyber-stalker cannot read

SoftPKeyMO, SoftPLocMO and SoftPEveMO. A Cyber-stalker cannot insert/delete SoftPArMO and SoftPTwtMO. A Friend cannot delete SoftPArMO and SoftPTwtMO. Finally, A Related cannot delete SoftPArMO.

```
fact{
//Readby Constraints on Soft Privacy data set
SoftPKeyMO.readby!=SC
SoftPLocMO.readby!=SC
SoftPEveMO.readby!=SC
//Insertby constraints on Soft Privacy data set
SoftPArMO.insertby!=SC
SoftPTwtMO.insertby!=SC
//Deleteby constraints on Soft Privacy set
SoftPArMO.deleteby!=SF
SoftPArMO.deleteby!=SR
SoftPTwtMO.deleteby!=SF
SoftPArMO.deleteby!=SC
SoftPTwtMO.deleteby!=SC
}
```

Section 9 Constraints on Soft Privacy.

Table 5 lists the user group according to each level.

Table 4. User group according to each level.

Low privacy users group	Description	Soft privacy users group	Description
LO	Low Privacy Owner	SO	Soft Privacy Owner
LR	Low Privacy Related	SR	Soft Privacy Related
LF	Low Privacy Friend	SF	Soft Privacy Friend
LC	Low Privacy Cyber-stalker	SC	Soft Privacy Cyber-stalker
Hard privacy users group	Description	Full privacy users group	Description
HO	Hard Privacy Owner	FO	Full Privacy Owner
HR	Hard Privacy Related	FR	Full Privacy Related
HF	Hard Privacy Friend	FF	Full Privacy Friend
HC	Hard Privacy Cyber-stalker	FC	Full Privacy Cyber-stalker

Figure 1 displays the metal model of MOP. It shows that "PrivacyDS" contains four subsets which are FullIP, HardP, LowP and SoftP. Each attribute from Keyword, URL, Location, Event, Articles, Tweets, and Username extends from each Privacy level. The privacy data are read by the different types of users which are Lusers, Susers, Husers and Fusers. Each type of user extends to Owner, Related, Friend and Cyber-stalker.

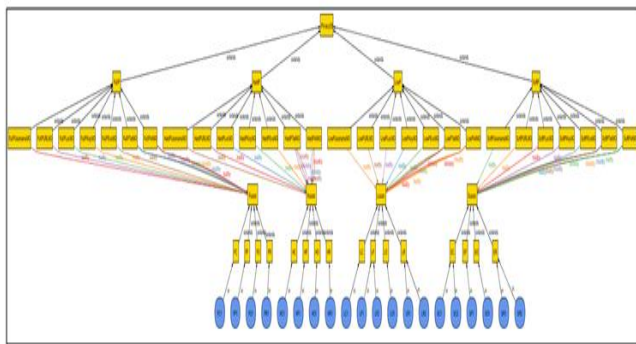


Figure 1. MOP Meta Model.

The model shows that the predicate is consistent, and an instance is found, as shown in figure 2. Figure 3 depicts that a Friend in the hard privacy is allowed to insert tweets for any multimedia

objects. One instance is shown below out of many that could be produced if next button is pressed using Alloy Analyzer.

```
Executing "Run test"
Solver=sat4j Bitwidth=0 MaxSeq=0 SkolemDepth=1 Symmetry=20
343 vars. 196 primary vars. 261 clauses. 168ms.
Instance found. Predicate is consistent. 80ms.
```

Figure 2. MOP consistency output using Alloy Analyzer.

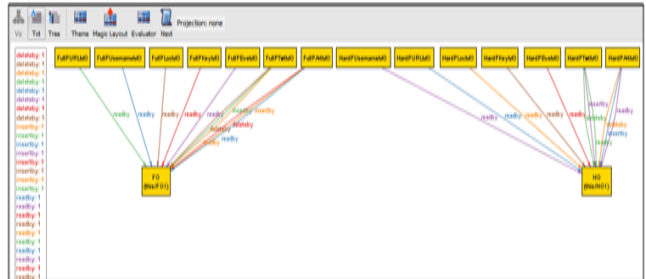


Figure 3. MOP model instance 1 (part 1).

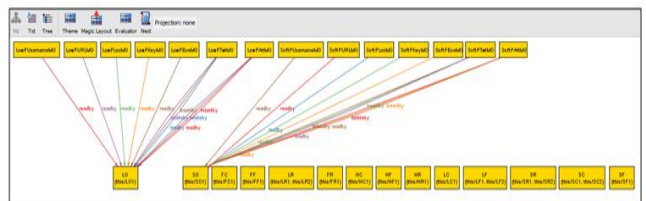


Figure 3. MOP model instance 1 (part 2).

After checking that the system is consistent, Section 10 is a counter example to validate that the model has worked as intended.

```
//Run Example to show Consistencies and inconsistencies
pred test()
{
HardPArMO.insertby=HF
}
run test
```

Section 10 MOP inconsistent predicate.

As shown in Figure 5, there was no inconsistency found; hence, the model's functionality executed as planned.

```
Executing "Run test"
Solver=sat4j Bitwidth=0 MaxSeq=0 SkolemDepth=1 Symmetry=20
0 vars. 0 primary vars. 0 clauses. 6ms.
No instance found. Predicate may be inconsistent. 0ms.
```

Figure 4. MOP inconsistent output using Alloy Analyzer.

5. CONCLUSION

In this paper, we proposed a multimedia object privacy model. MOP tackles the main security issues that the user is unaware of when publishing any multimedia object like images, videos, audio tracks and so on. The model expresses multimedia objects using seven main entities - keyword, URL, Event, Location, Tweets, Articles and Username. These entities formed the multimedia object in order to give the owner the flexibility to enforce restrictions on some entities while providing access to the others depending on the type of users accessing the object. System examples were executed based on the constraints applied on the

four security levels: Low, Soft, Hard, and Full privacy. The consistencies and inconsistencies of the model were accomplished by the Alloy Analyzer tool that is based on first-order logic, which means the system is expressed as Boolean functions to be checked for correctness. Counter examples were shown to guarantee that the model is functioning as planned.

In the future, the plan is to enhance the model by combining the MOP model with the Role-Based Access Control mechanism in order to achieve a complex privacy for improved security of the user's data and information.

6. REFERENCES

- [1] Jackson, D. 2002. D. Jackson. Alloy: a lightweight object modeling notation. *ACM Transaction on Software Engineering and Methodology (TOSEM)*, 11(2):256–290.
- [2] Aïmeur, E., Gambs, S., & Ho, A. 2009. UPP: user privacy policy for social networking sites. In *Proceedings of the IEEE Fourth International Conference Internet and Web Applications and Services, (ICIW '09)*, 267- 272. Montreal, QC, 267-272.
- [3] Al Bouna, B., Raad, E. j., Elia, C., Chbeir, R., & Haraty, R. 2013. de-Linkability: a privacy-preserving constraint for safely outsourcing multimedia documents. In *Proceedings of the International ACM Conference on Management of Emergent Digital EcoSystems (MEDES 2013)*. Neumunster Abbey, Luxembourg.
- [4] Joshi, J., Aref, W., Ghafoor, A., & Spafford, E. 2001. Security models for web-based applications. *Communications of the ACM*, (Feb. 2001), 38-44.
- [5] Joshi, J. B., Kevin Li, Z., Fahmi, H., Shafiq, B., & Ghafoor, A. 2002. A model for secure multimedia document database system in a distributed environment. *IEEE Transactions on Multimedia*, volume 4, issue 2, 215-234.
- [6] Kodali, N., Farkas, C., & Wijesekera, D. 2004. An authorization model for multimedia digital libraries. *International Journal on Digital Libraries*, 4: / Digital Object Identifier (DOI) 10.1007/s00799-004-0080-1, 139-155.
- [7] Hangzai Luo, J. F., Hacid, M., & Bertino, E. 2005. A novel approach for privacy-preserving video sharing. In *Proceedings of the CIKM Confernece*, Bremen, Germany, 609-616.
- [8] Lian, S., Kanellopoulos, D., & Ruffo, G. 2009. Recent advances in multimedia information system security. *Informatica 33*, 3-24.
- [9] Ridzon, R., & Levicky, D. 2009. Multimedia security and multimedia content protection. In *Proceedings of the International Symposium ELMAR*, Zadar, Croatia, 104-109.
- [10] Al Bouna, B., Chbeir, R., & Marrara, S. 2009. Enforcing role based access control model with multimedia signatures. *Journal of Systems Architecture*, volume 55, issue 4, 264-274.
- [11] Al Bouna, B., Chbeir, R., & Gabillon, A. 2011. The image protector: a flexible security rule specification toolkit. In *Proceedings of the International Conference on Security and Cryptography*. Seville, Spain.
- [12] Saad, S., Al Bouna, B., & Chbeir, R. 2011. Privacy preserving via tree augmented naive Bayesian classifier in multimedia databases. In *Proceedings of the ACM Conference on Management of Emergent Digital EcoSystems (MEDES 2011)*, San Francisco, USA, 297-204.
- [13] Ben Dhia, I., Abdessalem, T., & Sozio, M. 2012. Primates: A privacy management system for social networks. In *Proceedings of the ACM CIKM'12 Conference*, Maui, HI, USA, 2746-2749.
- [14] Zhuo, L., Diao, M., Zhang, J., & Li, Z. 2013. Hierarchical privacy preservation for personalized image retrieval. In *Proceedings of the ACM ICIMCS Conference*, Huangshan, Anhui, China, 291-295.
- [15] Netscape. (1998, June 5). *DMOZ*. Retrieved April 20, 2014, from wikipedia: <http://en.wikipedia.org/wiki/DMOZ>.
- [16] Panda, B., Perrizo, W., & Haraty, R. A. 1994. Secure transaction management and query processing in multilevel secure database systems. In *Proceedings of the ACM Symposium on Applied Computing*. Phoenix, AZ, USA, 363-368.
- [17] Haraty, R. A., & Massalkhy, S. 2013. UPP+: A flexible user privacy policy for social networking services. *Security and Privacy Preserving in Social Networks*. Springer-Verlag Wien. ISBN 978-3-7091-0893-2.
- [18] Haraty, R. A., Naous, M., & Mourad, A. 2014. Assuring Consistency in Mixed Models. *Journal of Computational Science*. ISSN: 1877 - 7503. 10.1016/j.jocs.2014.02.009, 653-663.