International Journal of Cloud Applications and Computing
Volume 11 • Issue 2 • April-June 2021

A Novel Spatio-Temporal Access Control Model for Online Social Networks and Visual Verification

Lanfang Zhang, College of Information Engineering, Henan University of Science and Technology, China & Henan International Joint Laboratory of Cyberspace Security Applications, Henan University of Science and Technology, China

Zhiyong Zhang, College of Information Engineering, Henan University of Science and Technology, China & Henan International Joint Laboratory of Cyberspace Security Applications, Henan University of Science and Technology, China

Ting Zhao, College of Information Engineering, Henan University of Science and Technology, China & Henan International Joint Laboratory of Cyberspace Security Applications, Henan University of Science and Technology, China

ABSTRACT

With the rapid development of mobile internet, a large number of online social networking platforms and tools have been widely applied. As a classic method for protecting the privacy and information security of social users, access control technology is evolving with the spatio-temporal change of social application requirements and scenarios. However, nowadays there is a lack of effective theoretical model of social spatio-temporal access control as a guide. This paper proposed a novel spatio-temporal access control model for online social network (STAC) and its visual verification, combined with the advantages of discretionary access control, using formal language to describe the access control rules based on spatio-temporal, and real-life scenarios for access control policy description, realizes a more fine-grained access control mechanism for social network. By using the access control verification tool ACPT developed by NIST to visually verify the proposed model, the security and effectiveness of the STAC model are proved.

KEYWORDS

ACPT, Online Social Network, Security, Spatio-Temporal Access Control, Visual Verification

INTRODUCTION

With the rapid development of online social network, online social networking platforms, tools and applications such as Twitter, Facebook, LinkedIn, QQ and WeChat are constantly penetrating into people's production, life and social activities (Pang et al., 2015; Liu et al., 2019). Users spend a lot of time on online social networking and communication every day, and a large amount of social data and information spread through online social network (Yin et al., 2019; Zhang, et al, 2019). In the environment of social big data, user data has a stronger correlation than before. With the increase of data, user information is correlated and matched. Compared with the traditional Internet environment, it becomes easier to access, collect and disseminate users' information, and users cannot effectively

DOI: 10.4018/IJCAC.2021040102

Copyright © 2021, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

control their personal information. While enjoying the convenience of social tools, users also faced with such problems as unauthorized access, data theft, information fraud, personal privacy disclosure, etc. Social network information access control has become a concern of people (Ma et al., 2019; Yamaguchi et al., 2019; Gupta, et al, 2019). Therefore, users need to effectively protect and supervise personal information through privacy protection technology at the source (Luo et al., 2018). As a classic method of information security and privacy protection, access control technology can be used to formulate complete rules and policies for different social scenarios of users. Such technology is the key technical guarantee for achieving virtual cyberspace security (Hu et al., 2013; Ahmed et al., 2016; Gupta, et al, 2018). In the online social network environment, the existing access control model distinguishes access subjects and objects based on user roles (Ulltveit et al., 2016), attributes (Wei et al., 2018), relationships (Cheng et al., 2016; Bui et al., 2019; Chen et al., 2014), tags (Zhang et al., 2016), groups (Hu et al., 2018), and so on, and it also describes and imposes visitor's access rights and operations to different resources.

With the continuous emergence of new scenarios and applications of online social network (Zheng,et. al, 2019; Sahoo, et. al, 2019), practical applications, such as security control mechanisms (Fang et al., 2017) and personal privacy protection (Ma et al., 2017), have appeared. Literature (Xue et al., 2018) and (Baseri et al., 2018) propose an attribute-based location-aware access control mechanism in the cloud environment, which flexibly combines user attributes and location to achieve fine-grained control of data. Literature (Hsu et al., 2016) and (Li et al., 2016) propose an access control model based on location attribute awareness in the social network, and verify the feasibility of user behavior through location attributes and fine-grained control of access to users' sensitive location information in shared content. Literature (Yang et al., 2016) suggests a provably secure access control scheme based on time domain attributes in the cloud environment, allowing users to decrypt video content within a specific time period. Literature (Fan et al., 2017) proposes a mandatory access control model with space-time constraints in the collaborative environment, according to BLP model, tasks, time, and space are considered.

The widespread and in-depth application of social network constantly changes user needs. Moreover, the following new scenarios emerge:

Scenario 1: Alice posts a group of funny pictures on the social network platform, but the picture content is related to personal privacy. She hopes that the pictures could be seen by friends only for a while for entertainment, and she wants to delete the pictures after 24 hours.

Scenario 2: Bob publishes detailed information of his lost item on the social network platform, hoping to retrieve it through the platform. However, he only wants this information to be seen by friends in his city.

Scenario 3: Charlie's relatives had lost and he posted a notice on social network. He hopes that his friend can currently browse the post and plans to delete it within 24 hours. At the same time, only friends in the same city can browse the information.

Given the spatio-temporal characteristics of online social network, social platform applications need fine-grained access control rules and policies to ensure the security of social big data and personal privacy (Hu et al., 2016). However, these related works is insufficient for the emerging new scenario, especially for lacking of the theoretical model of Spatio-Temporal Access Control (STAC). Our research motivation is to propose a novel access control model for online social networks and realize its visual verification. The main contribution focus on considers temporal and spatial factors comprehensively. Such a feature provides access to control modeling and theoretical guidance for the increasing social network application scenarios.

The rest of this paper is organized as follows. Section 2 proposes the construction and formal description of STAC model. Section 3 describes the spatio-temporal access control rules of STAC model. Based on the above rules, security policies of the given social application scenarios are

described in Section 4. Finally, Section 5 carries out instrumental verification and comparative analysis of STAC model proposed in this article; finally, the conclusion, looking forward to the next step.

CONSTRUCTION AND FORMAL DESCRIPTION OF STAC MODEL

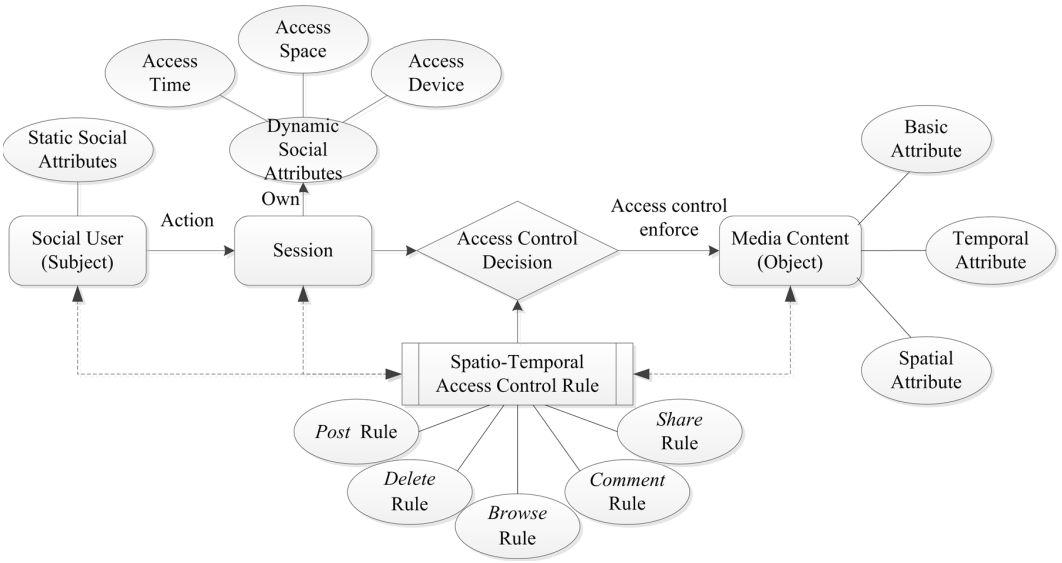
In the STAC model, the access requester is the user, and the object is the media content. First, the user initiates an access request to the media content and simultaneously activates the session. Each user contains static attributes. After activating the session, the access control decision module extracts the static social attributes and dynamic social attributes of the access user. Accordingly, the module then decides whether to grant permissions based on the spatio-temporal access control rules set by the object. Figure 1 shows the STAC model framework, which contains the basic components of social users, media content, session, social situation, spatiotemporal access control rules, information flow control rules, and decision module.

The STAC model can be represented by a sextuple (*U, O, A, T, S, E*), which includes the following components:

- $U=\{u_1, u_2,..., u_n\}$ is a set of subjects (users in online social networks);
- $O=\{o_1, o_2,..., o_n\}$ is a set of objects (media content for information sharing in online social networks);
- $A=\{a_1, a_2,..., a_n\}$ is a set of operations (behaviors) by a subject in an online social network;
- $T=\{t_1, t_2,..., t_n\}$ is a set of time points when the subject visits the object;
- $S=\{s_1, s_2,..., s_n\}$ is a set of physical spatial location points; and
- $E=\{m, n\}$ indicates a set of access devices (including mobile and non-mobile).

Definition 1 - Identity (ID): Each subject (object) has a unique identity *ID*, and the identity of the subject *ID* is expressed as $SID=\{s.id_1, s.id_2,..., s.id_n\}$ (where *n* represents the number of subjects in the model). The identity of all objects *ID* is expressed as $OID=\{o.id_1, o.id_2,..., o.id_n\}$ (where *n* is the number of objects in the model).

Figure 1. Access control model of online social network based on spatio-temporal (STAC)



Definition 2 - Security Level (SL): (*SL*) Each subject (object) contains security level attribute *s.SL* (*o.SL*), and the security level can be expressed as $SL=\{SL_1, SL_2,..., SL_n\}$ (where *n* is the number of security levels in the model), $SL_{min} \leq SL_i \leq SL_{max}$, and SL_{min} and SL_{max} are the minimum and maximum security levels, respectively. The partial-order relationship between security levels can be expressed as $SL_i \leq SL_j$,$(SL, \leq)$, which forms a bounded lattice.

Definition 3 - Momentary Access Period (T_M): Each object contains a temporary access period attribute, $o.T_M$, which is between the time point when a subject accesses and the time point when the subject access is forbidden. The temporary access time interval can be expressed as $T_M=\{T_{M1}, T_{M2},..., T_{Mn}\}$. That is, the access start time and prohibited access time of a subject to the object are T_{Msi}, T_{Mei}, $T_{Mi}=T_{Mei}-T_{Msi}$ (where $T_{Msi} \leq T_{Mei}$).

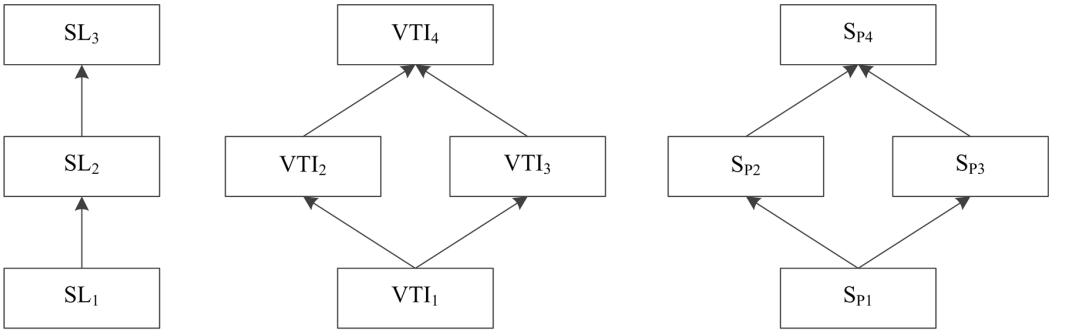
Definition 4 - Valid Time Interval (VTI): Each object contains an effective interval attribute *o.VTI* that allows access by any subject. The effective interval can be expressed as $VTI=\{VTI_1, VTI_2,..., VTI_n\}$, $VTI_i=[VTI_{si}, VTI_{ei}]$, where VTI_{si} and VTI_{ei} represent the time points when the object is published and when access is allowed to end (where $VTI_{si} \leq VTI_{ei}$), respectively. The partial-order relationship between effective intervals can be expressed as $VTI_{ei} \subseteq VTI_{ei}$ (where $VTI_i=[VTI_{si}, VTI_{ei}]$, $VTI_j=[VTI_{sj}, VTI_{ej}]$, $VTI_{sj} \leq VTI_{si}$ and $VTI_{ei} \leq VTI_{ej}$), and $(VTI, \subseteq)$ forms a bounded lattice.

Definition 5 - Physical Space Scope (S_p): Each object contains the physical space scope attribute $o.S_P$ that the subject can access. The physical space scope can be expressed as $S_P=\{S_{P1}, S_{P2},..., S_{Pn}\}$. Each physical space scope $S_{Pi}=\{S_{Pi1}, S_{Pi2},..., S_{Pin}\}$ is a set of several physical space position points. The partial-order relationship among physical space scopes can be expressed as $S_{Pi} \propto S_{Pj}$,$(S_P, \propto)$, which forms a bounded lattice.

This paper uses the operators "$\leq$", "$\subseteq$" and "$\propto$" to indicate the partial-order relationship among security level, valid time interval, and physical space scope. A unique maximum lower bound is found in the set of security levels, valid time intervals, and physical space scopes, which are governed by all other access classes in the set. A unique minimum upper bound governs other access classes in the set. The three attribute sets *SL*, *VTI*, and S_P form bounded lattices, respectively, with the operators "$\leq$", "$\subseteq$" and "$\propto$". The three partial order relationships are shown in Figure 2.

Example 1: Figure 2(a) is the partial ordering relation between security levels on $SL=\{SL_1, SL_2, SL_3\}$, where $SL_1 \leq SL_2$,$SL_2 \leq SL_3$. In the practical application of online social networks, friends can be divided into three security levels from high to low, i.e., {friends, friends-of-friends, friends-of-friends-of-friends}, and the value of each level is expressed as 1, 2, and 3.

Figure 2. Partial ordering relation among security levels, valid time intervals, and physical space scopes of STAC model



(a) Security Levels (b) Valid Time Intervals (c) Physical Space Scopes

Example 2: Figure 2(b) is the partial order relationship among valid time intervals on $VTI=\{VTI_1, VTI_2, VTI_3, VTI_4\}$, where $VTI_1 \subseteq VTI_2$, $VTI_1 \subseteq VTI_3$, $VTI_2 \subseteq VTI_4$, $VTI_3 \subseteq VTI_4$. Assume that the unit of time used by the online social network system is day, and an example is given that can satisfy some examples VTI_1=[2018/10/01, 2019/12/31], VTI_2=[2018/03/01, 2020/05/01], VTI_3=[2018/05/01, 2020/10/01], and VTI_4=[2018/01/01, 2020/12/31].

Example 3: Figure 2(c) is the partial order relationship among spatial scopes on $S_P=\{S_{P1}, S_{P2}, S_{P3}, S_{P4}\}$, where $S_{P1} \propto S_{P2}$, $S_{P1} \propto S_{P3}$, $S_{P2} \propto S_{P4}$, and $S_{P3} \propto S_{P4}$. We take an example that can satisfy some orders, S_{P1}={ United States}, S_{P2}={ United States and Mexico}, S_{P3}={ United States and Canada}, and S_{P4}={ North America}.

Definition 6 - Access Equipment (E): Each object contains the attributes of the access device used by the subject. The access device can be expressed as $E=\{m, n\}$, where m is mobile, and n is non-mobile.

Definition 7 - Action (A): The operation (behavior) that each subject can initiate on the object can be expressed as $A=\{Post, Delete, Browse, Comment, Share\}$, that is, the behavior includes posting, deleting, browsing, commenting, and sharing. In the access control model, these behaviors are completed by the state transition function, and the subject transitions from one state to another by calling the state transition function. The state transition function is defined as follows:

- $Post(u, o, SL, T_M, VTI, S_P, E, t_0)$: The subject u publishes an object o with the security level of SL, momentary access period of T_M, valid time interval of VTI, physical space scope of S_P, and access device of E;
- $Delete(u, o, t_0)$: The subject u deletes the object o at t_0;
- $Browse(u, o, t_0)$: The subject u browses the object o at t_0;
- $Comment(u, o, t_0, SL, v)$: The subject u comments the object o at t_0, generating version v with the security level of SL;
- $Share(u, o, t_0, SL, T_M, VTI, S_P, E, v)$: The subject u shares the object o, generating version v with the security level of SL, momentary access period of T_M, valid time interval of VTI, physical space scope of S_P, and access device of E.

Definition 8 - Information Flow: When the subject accesses the object, a corresponding information flow is generated, and the symbol "→" indicates the flow of information. Information flow is controlled according to the partial order relationship between the defined security levels, valid time intervals, and physical space scopes. This paper uses information flow to ensure the flow direction of information. Through information flow control rules, we observe how information flows from one subject (object) to another. When the subject u browses object o, the information flows from the object o to the subject u; when the subject u comments at object o and generates version v, the information flows from the subject u to object v; when the subject u shares object o and generates a new version v', information flows from object o to version v'.

Definition 9 - Access Control Rule Set (RS): RS is a set of all access control rules in an access control system. Among them, $RS_i \in RS(i=1, 2,\ldots, n)$ describes the access control rules of action A performed by subject u on object o (n represents the number of access control rules in the system). The access control rules are provided by the function RS_i: $accept \leftarrow condition$ for definition and judgment, where "*condition*" is a logical operation expression, connected by operators "∧" and "∨." If the function is established (the object o accepts the access operation A of the subject u), that is, the "*condition*" logical expression is accepted, each expression in the logical expression needs to be satisfied. Otherwise, access is denied. After the access, access operations will change the attributes or relationships between the subject (user) and object. Hence, RS_{ei} (where $i=1, 2,\ldots, n$) is used to describe the results after access, where n represents the number of access control rules in the system.

STAC MODEL SPATIO-TEMPORAL ACCESS CONTROL RULES

Present your perspective on the issues, controversies, problems, etc., as they relate to theme and arguments supporting your position. Compare and contrast with what has been, or is currently being done as it relates to the article's specific topic and the main theme of the journal.

According to the definition of state transition function, the access control rules of STAC model are described formally. The state transition function describes the change of system security state caused by the change of the value of security state.

In the access control rule, U_o is used to represent the set of objects created by the subject u, and O_v represents the set of versions of object o. $o.oid$ and $v.oid$ represent the original owner of the object o and the original object of version v, respectively. Meanwhile, the tree tr is introduced, *create_tree(tr, root, o.id)*, *add_child_tree(tr, o.id, node*$_1$*, v*$_1$*.id, node*$_2$*, v*$_2$*.id)*, and *delete_tree(tr, o.id)* mean to create a tree *tr rooted as o.id*; a $node_2$ with the value of $v_2.id$ is added to a child node $node_1$ (the root is $v_1.id$) on the tree tr (the root is $o.id$); and the tree tr with the root $o.id$ of is deleted.

In the following rules, the subject u is not necessarily the owner of object o, and object o may not be the original object (may be a new version object shared by other subjects).

Rule 1: (*Post* rule) At t_0, the subject u publishes an object o with the security level of SL_0, momentary access period of T_{M0}, valid time interval of VTI_0, physical space scope of S_{P0}, and access device of e; where SL_0 is constrained by the minimum upper bound and maximum lower bound of the partially ordered set SL; valid time interval starts at t_0, and momentary access period T_{M0} is shorter than the access period of valid time interval VTI_0=[t_0, VTI_{0e}]. After completing *Post* operation, object o is included in the list of subject u (the root of the tree tr $o.id$ is o itself); original subject of the object o is u, and the original version is v_0. The version set of the object o contains the version v_0 and creates a tree tr with a root of $o.id$. Rule 1 can be written as follows:

$$RS_1 : accept \leftarrow (a = Post(u, o, SL_0, T_{M0}, VTI_0, S_{P0}, E, t_0))$$
$$\wedge (o.SL = SL_0) \wedge (o.T_M = T_{M0}) \wedge (o.VTI = VTI_0)$$
$$\wedge (T_{M0} \leq VTI_{0e} - t_0) \wedge (o.S_P = S_{P0}) \wedge (E = e)$$
$$\wedge (SL_{\min} \leq o.SL \leq SL_{\max})$$
$$RS_{e1} : o \in U_o, o.oid = u, v.oid = v_0, v_0 \in O_v,$$
$$creat\_tree(tr, root, o.id)$$

In the above rule, SL_0, T_{M0}, VTI_0, and S_{P0} are set by the user (or recommended by the system and ultimately decided by the user). In Section 4, we discuss how to define the initial values SL, T_M, VTI, and S_P in real application.

Rule 2: (*Delete* rule) At the time point t_0, the subject u deletes object o. The condition to be satisfied is that the subject u is the owner of object o (where object o may not be the original object, but it must be the subject posted or shared by the subject u), and the subject o has been posted at t_0. After completing *Delete* operation, object o is not in the list of the subject u, and the ending time of valid time interval of object o is t_0. When deleting the version set of object o, all the versions of object o in $tr_{o.oid}$ are deleted, where tree $tr_{o.oid}$ is composed of the last *Post* and *Share* operations. Rule 2 can be written as follows:

$RS_2 : accept \leftarrow (a = Delete(u, o, t_0))$
$\wedge(o \in U_o) \wedge (o.oid = u) \wedge (t_0 \in o.VTI)$
$RS_{e2} : o \notin U_o, o.VTI = [o.VTI.VTI_s, t_0], delete(O_v),$
$(for\ all\ \mathrm{v} \in tr_{o.id}, delete(v))$

Rule 3: (*Browse* rule) At time point t_0, the subject *u* browses the object *o*. The condition to be satisfied is that the security level of the subject *u* is not lower than that of the object *o*, and time t_0 is within the valid time interval of object *o*. In addition, physical space location point is included in the physical space scope attribute of the object *o*, and the access device is the access device *e* for the object. After completing *Browse* operation, the set of points in time when the subject *u* can access the object *o* starts from t_0 and ends at t_0 plus the momentary access period and the end time of the valid time interval. The information flows from the object *o* to the subject *u*. Rule 3 can be written as follows:

$RS_3 : accept \leftarrow (a = Browse(u, o, t_0))$
$\wedge(o.SL \leq u.SL) \wedge (t_0 \in o.VTI) \wedge (u.s \in o.S_P) \wedge (E = e)$
$RL_{e3} : T = [t_0, \min\{t_0 + o.T_M, o.VTI.VTI_e\}], o \rightarrow u$

Rule 4: (*Comment* rule) At time point t_0, the subject *u* comments at object *o*. The condition to be satisfied is that the information can flow from object *o* to the subject *u*, i.e., the subject *u* can read object *o*, which conforms to Rule 3. At the same time, the security level of the new version v generated after the comment is defined as SL_v, and the security level of *v* is not lower than that of the comment subject *u* and not higher than the minimum upper bound of the partially ordered set of *SL*. After *Comment* operation, a new version *v* of object *o* is created, in which the version set of object *o* includes version *v*, and the momentary access period is the same with that of object *o*. The valid time interval starts from the current time t_0, with the ending time the same with that of valid time interval of object *o*, and the physical space scope of version *v* is the same with that of object *o*. Rule 4 can be written as:

$RS_4 : accept \leftarrow (a = Comment(u, o, t_0, SL_v, v))$
$\wedge(\exists o \rightarrow u) \wedge (v.SL = SL_v) \wedge (u.SL \leq SL_v \leq SL_{\max})$
$RS_{e4} : v \in O_v, v.T_M = o.T_M, v.VTI = [t_0, o.VTI.VTI_e], v.S_P = o.S_P$

Rule 5: (*Share* rule) At the time point t_0, the subject *u* shares object *o* (the version of object *o* may not be the original version v_0) and creates new version *v*. The condition to be satisfied is that the information can flow from the object *o* to the subject *u*, i.e., the subject *u* can read object *o*, which conforms to Rule 3. At the same time, the security level of the new version v generated after the comment is defined as SL_v, and the security level of *v* is not lower than that of the comment subject *u* and not higher than the minimum upper bound of the partial ordering set of *SL*. The momentary access period of version *v* is not greater than that of the object *o*. The valid time interval starts from the current time t_0, and the ending time is not greater than the end of valid time interval time of object *o*. The physical space scope of version *v* is included in the space scope of object *o*, and its access device is included in the access device of object *o*. After completing *Share* operation, the subject *u* creates a new version *v*. The version set of object *o* includes version *v*, which is added to the tree *tr* (the root is *o.oid*), with the node of $node_2$ (value

is *v.id*). The parent node is the $node_1$ of object *o* (value is *o.id*), and the information flows from subject *u* to object *v*. Rule 5 can be written as:

$$RS_5 : accept \leftarrow (a = Share(u, o, t_0, SL_v, T_{Mv}, VTI_v, S_{Pv}, E, v))$$
$$\wedge(\exists o \rightarrow u) \wedge (v.SL = SL_v) \wedge (u.SL < \mathrm{SL}_v \leq SL_{\max})$$
$$\wedge(v.T_M \leq o.T_M) \wedge (v.VTI = [t_0, v.VTI.VTI_e])$$
$$\wedge(v.VTI.VTI_e \leq o.VTI.VTI_e) \wedge (v.S_P \subseteq o.S_P) \wedge (v.E \subseteq o.E)$$
$$RS_{e5} : v \in O_v, u \rightarrow v, add\_child\_tree(tr, o.oid, node_1, o.id, node_2, v.id)$$

DESCRIPTION OF MODEL STRATEGY IN APPLICATION SCENARIOS

In this section, for the specific application scenarios exemplified in Chapter 1, policy analysis is performed by the spatio-temporal access control rules in Chapters 3. Next, access control policies are set according to three scenarios.

Scenario 1: Alice posts her funny photos on the platform, but she hopes that they would disappear immediately after her friends browse them, and the system could delete the photos automatically 24 hours after they are posted. Then, when Alice posts the photos, she needs to limit the momentary access period to 5 seconds, the valid time interval to 24 hours, and the access device to be a mobile terminal. According to Alice's needs and control rules, we set access control policy 1:

$$P_1 : accept \leftarrow (a = Post(u, o, SL_0, T_{M0}, VTI_0, S_{P0}, E, t_0))$$
$$\wedge(o.T_M = 5s) \wedge (o.VTI = [t_0, t_0 + 24h]) \wedge (E = m)$$

Scenario 2: After Bob posts information about his lost items on the platform, he hopes that only friends in the same city could see this information. Then, when Bob posts the information, he needs to set the spatial scope to "Visible in the Same City," and the access device to be a mobile terminal. According to Bob's needs and control rules, we set access control policy 2:

$$P_2 : accept \leftarrow (a = Post(u, o, SL_0, T_{M0}, VTI_0, S_{P0}, E, t_0))$$
$$\wedge(o.S_P = "Visible\ in\ the\ Same\ City") \wedge (E = m)$$

Scenario 3: Charlie posts information on the platform, but he hopes that the post would be deleted automatically after 24 hours, disappear immediately after browsing, and only accessible within the same city. Then, when David posts the information, he needs to limit the momentary access period to 5 seconds, valid time interval to 24 hours, spatial scope to "Visible in the Same City," and the access device is a mobile terminal. According to Charlie's needs and control rules, we set access control policy 3:

$$P_4 : accept \leftarrow (a = Post(u, o, SL_0, T_{M0}, VTI_0, S_{P0}, E, t_0))$$
$$\wedge(o.T_M = 5s) \wedge (o.VTI = [t_0, t_0 + 24h])$$
$$\wedge(o.S_P = "Visible\ in\ the\ Same\ City") \wedge (E = m)$$

According to the description of the above three application scenarios and the setting of the access control policy for each scenario, STAC model proposed in this article controls the time and space of

information access. Through more fine-grained access control policy settings, the privacy of social users is ensured. Hence, the proposed model is fine-grained, dynamic, and controllable.

VISUAL VERIFICATION AND COMPARATIVE ANALYSIS OF ACCESS CONTROL MODEL

Visual Verification of Access Control Model

The Access Control Policy Tool was developed by the National Institute of Standards and Technology NIST, which can simulate different access control policies and policy environments (Hu et al., 2016). ACPT provides GUI templates for composing access control models, NuSMV (Symbolic Model Verification) model checker to verify the security requirements of access control models through symbolic model verification, Generated by NIST's combination testing tool ACTS The complete test case of XACML strategy generates the output as a verified model. ACPT performs all grammatical and semantic verification through these four main functions, as well as an interface for writing and combining access control models for access control strategies; ACPT ensures the efficiency of specifying access control models and eliminates the manufacturing of defective AC models and the possibility of leaking information or prohibiting legal information sharing.

The STAC model proposed in this article rules are input into the ABAC model framework, as shown in Figure 3 (a), and the access control strategies of the three realistic scenarios are input into the WorkFlow model framework, as shown in Figure 3 (b). The ABAC model framework and the WorkFlow model framework separately verify the security of access control rules and real-world scenario policies. The rule verification is showed in Figure 4 (a), and the three scenarios are shown in Figure 4 (b), Figure 4 (c) and Figure 4 (d). Test cases are obtained and XACML files are exported.

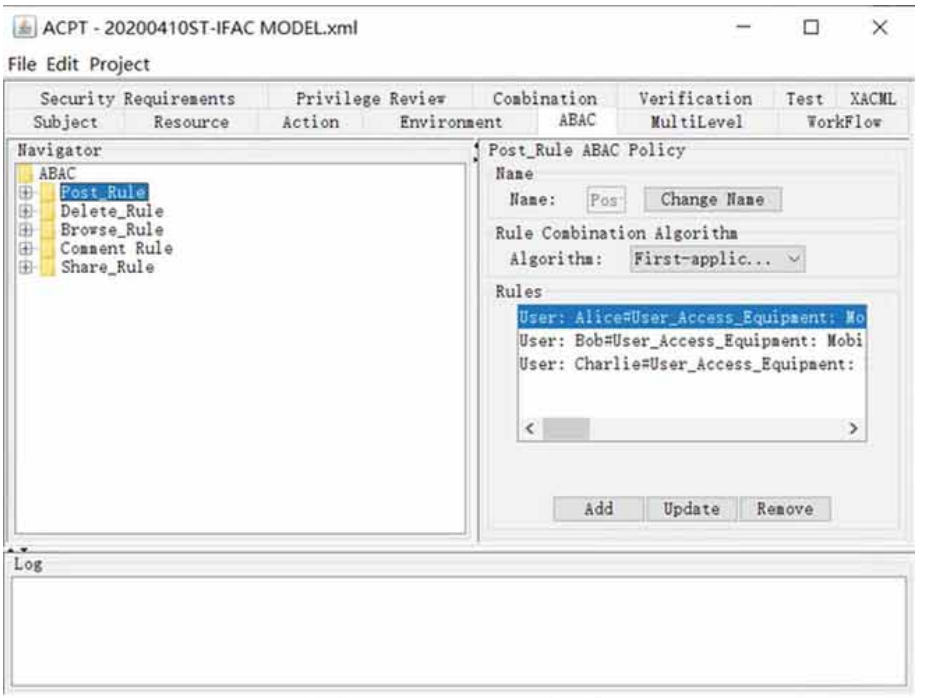
The STAC model proposed in this paper verifies the consistency and security of access control rules and access control strategies in real-world scenarios under the ABAC model framework and WorkFlow model framework of the ACPT tool, and generates test cases and XACML language files.

Comparative Analysis of Access Control Models

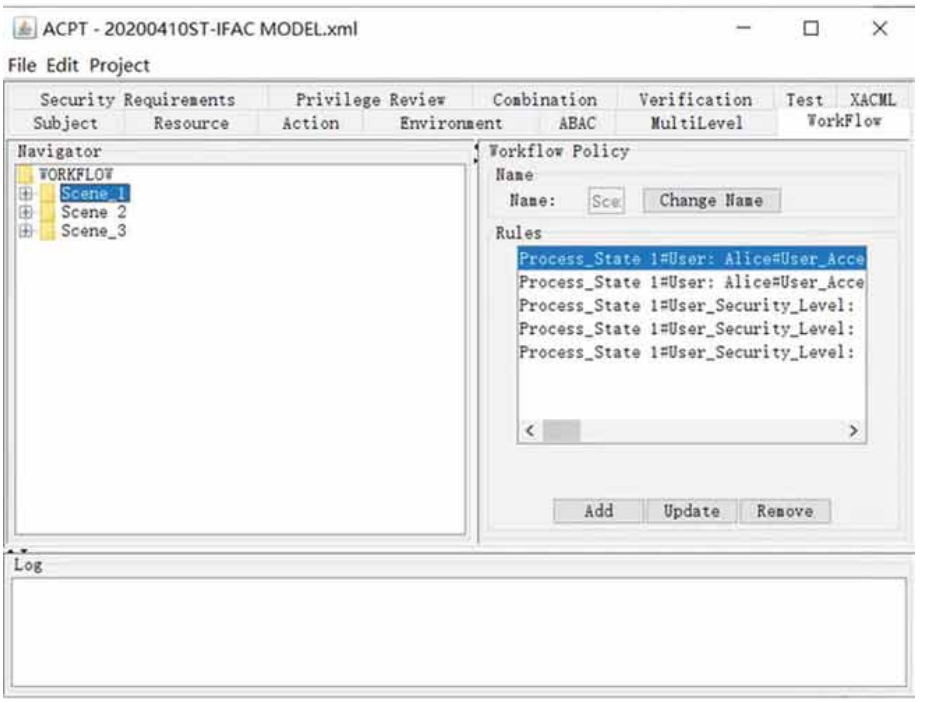
The STAC model proposed in this paper is compared with several access control models in the social network environment in Literature (Pang et al., 2015; Cheng et al., 2016; Chen et al., 2014; Han et al., 2016; Hu et al., 2018). As shown in Table 1, "$\surd$" means support Corresponding functional characteristics.

Reference (Pang et al., 2015) proposes an online social network access control model that includes users, user relationships, and public information for public information security issues. Reference (Cheng et al., 2016) for a variety of user relationship types, combined with two path inspection algorithms to determine whether the user has a relationship, proposed a user access control based on user relationship (UURAC) model. Literature (Chen et al., 2014) proposed an access control model for multimedia social network based on household type, closeness, content sharing depth and trust degree. There are no consideration given to the control of the user's dynamic attributes and environmental attributes. Literature (Han et al., 2016) proposed an attribute-based access control model ABAC-MSN under multimedia social networks, which comprehensively considers the relationship among user attributes, environment attributes, resource attributes, and users. Only multimedia access operations are considered, and no complex interactions such as comments, reposts, and sharing by users under social networks are considered. Literature (Hu et al., 2018) proposed a group-based access control (oGBAC) framework for online social network to prevent privacy leakage when sharing information within or between groups in OSNs. The oGBAC model lacks control of relationship depth and environmental attributes.

Figure 3. Setting access control rules and three scenario policies



(a) Setting access control rules



(b) Setting three scenario policies

Figure 4. Access control rule and three scenario verification

(a) Access control rule verification

(b) Scenario 1 policy verification

(c) Scenario 2 policy verification

(d) Scenario 3 policy verification

Table 1. Comparative analysis of access control models in social networks

Literature	Pang et al., 2015	Cheng et al., 2016	Chen et al., 2014	Han et al., 2016	Hu et al., 2018	This article
User Static Attributes	√	√	√	√	√	√
User Dynamic Attributes				√	√	√
Relationship Depth	√	√	√	√	√	√
Trust	√		√	√		
Resource Attribute	√	√	√	√	√	√
Multiple Operating Behaviors					√	√
Environmental attributes				√		√

CONCLUSION

The emerging and popularity of spatio-temporal essential factors under online social networks has put forward higher requirements for the access control modelling. This paper proposes a novel spatio-temporal access control model for online social networks (STAC) and its visual verification, which takes account time and space factors into consideration, and real-life scenarios for access control policy description, establishes a more fine-grained and dynamic access control mechanism for social network. By using the access control verification tool ACPT developed by NIST to verify the proposed model, the security and effectiveness of STAC model are proved. The proposed model is suitable for some complex scenarios of the emerging online social networks, such as security and privacy concerned applications, where the effective access control is crucial and indispensable. The next step is to explore social context security theory and the impact of potential intent of social users on the dynamic change of online social network access control modeling.

ACKNOWLEDGMENT

The work was sponsored by National Natural Science Foundation of China Grant No.61972133, Project of Leading Talents in Science and Technology Innovation for Thousands of People Plan in Henan Province Grant No.204200510021, Henan Province Key Scientific and Technological Projects Grant No.192102210130 and No.202102210162, and Key Scientific Research Projects of Henan Province Universities Grant No.19B520008. We show gratitude to the reviewers and editor for their valuable comments, questions and suggestions. Dr. Brij Gupta, editor in chief of the International Journal of Cloud Applications and Computing (IJCAC), affiliated with National Institute of Technology in Kurukshetra, India, aided with the completion of this project. He received PhD degree from Indian Institute of Technology Roorkee, India in the area of Information and Cyber Security. He published more than 250 research papers in International Journals and Conferences of high repute. He is also working as principal investigator of various R&D projects. Dr. Gupta is senior member of IEEE. He was also visiting researcher with several universities worldwide. At present, Dr. Gupta is working as Assistant Professor in the Department of Computer Engineering, National Institute of Technology Kurukshetra India. His research interest includes Information security, Cyber Security, Cloud Computing, Web security, Intrusion detection and Phishing. He can be contacted by the email: gupta.brij@gmail.com.

REFERENCES

Ahmed, H., & Mante, R. (2016). Location based privacy preserving access control for relational data. In *2016 IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology* (pp. 2083-2087). IEEE.

Baseri, Y., Hafid, A., & Cherkaoui, S. (2018). Privacy preserving fine-grained location-based access control for mobile cloud. *Computers & Security*, *73*, 249–265. doi:10.1016/j.cose.2017.10.014

Bui, T., Stoller, S., & Li, J. (2019). Greedy and evolutionary algorithms for mining relationship-based access control policies. *Computers & Security*, *80*, 317–333. doi:10.1016/j.cose.2018.09.011

Chen, Q., Zhang, Z., Xiang, F., & Wang, J. (2014). Research on access control model for multimedia social networks. *Journal of Xidian University*, *41*(6), 181–187.

Cheng, Y., Park, J., & Sandhu, R. (2016). An access control model for online social networks using user-to-user relationships. *IEEE Transactions on Dependable and Secure Computing*, *13*(4), 424–436. doi:10.1109/TDSC.2015.2406705

Fan, Y. (2017). Temporal-spatial-based mandatory access control model in collaborative environment. *Computer Science*, (8), 107–114.

Fang, L., Yin, L., Zhang, Q., Li, F., & Fang, B. (2017). Who is visible: resolving access policy conflicts in online social networks. In *2017 IEEE Global Communications Conference* (pp. 1-6). IEEE. doi:10.1109/GLOCOM.2017.8254015

Gupta, B. B. (Ed.). (2018). *Computer and cyber security: principles, algorithm, applications, and perspectives*. CRC Press.

Gupta, B. B., & Sheng, Q. Z. (Eds.). (2019). *Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices*. CRC Press. doi:10.1201/9780429504044

Hsu, A., & Ray, I. (2016). Specification and enforcement of location-aware attribute-based access control for online social networks. In *ABAC 2016 - Proceedings of the 2016 ACM International Workshop on Attribute Based Access Control* (pp. 25-34). ACM.

Hu, D., Hu, C., Fan, Y. Q., & Wu, X. (2018). oGBAC—A group based access control framework for information sharing in online social networks. *IEEE Transactions on Dependable and Secure Computing*, 1–18. doi:10.1109/TDSC.2018.2875697

Hu, H., Aah, G., & Jorgensen, J. (2013). Multiparty access control for online social networks: Model and mechanisms. *IEEE Transactions on Knowledge and Data Engineering*, *25*(7), 1614–1627. doi:10.1109/TKDE.2012.97

Hu, L., Huang, Z., Deng, F., Yan, K., & Liu, J. (2016). Towards a location aware semantic access control approach for mobile computing. In *2016 International Conference on Identification, Information and Knowledge in the Internet of Things* (pp. 485-490). IEEE. doi:10.1109/IIKI.2016.117

Hu, V., & Kuhn, R. (2016). Access Control Policy Verification. *Computer*, *49*(12), 80–83. doi:10.1109/MC.2016.368

Li, C., Yin, L., Geng, K., & Fang, B. (2016). Location privacy preservation approach towards to content sharing on mobile online social network. *Journal of Communication*, *37*(11), 31–41.

Liu, N., Jing, W., Song, W., & Zhang, J. (2019). Measurement method of carbon dioxide using spatial decomposed parallel computing. *International Journal of High Performance Computing and Networking*, *14*(1), 8–16. doi:10.1504/IJHPCN.2019.099741

Luo, E., Wang, G., Liu, Q., & Meng, D. (2018). Fine-grained secure friend discovery scheme in mobile social networks. *Journal of Software*, *29*(10), 3223–3238.

Ma, C., Yan, Z., & Chen, C. (2019). Scalable access control for privacy-aware media sharing. *IEEE Transactions on Multimedia*, *21*(1), 173–183. doi:10.1109/TMM.2018.2851446

Ma, L., Yang, W., Huo, Y., & Zhong, Y. (2018). Research on access control model of social network based on distributed logic. *Future Generation Computer Systems*, *83*, 173–182. doi:10.1016/j.future.2017.11.041

Pang, J., & Zhang, Y. (2015). A new access control scheme for facebook-style social networks. *Computers & Security*, *54*, 44–59. doi:10.1016/j.cose.2015.04.013

Sahoo, S. R., & Gupta, B. B. (2019). Classification of various attacks and their defence mechanism in online social networks: A survey. *Enterprise Information Systems*, *13*(6), 832–864. doi:10.1080/17517575.2019.1605542

Ulltveit, M., & Oleshchuk, V. (2016). Enforcing mobile security with location-aware role-based access control. *Security and Communication Networks*, *9*(5), 429–439. doi:10.1002/sec.879

Wei, J., Liu, W., & Hu, X. (2018). Secure and efficient attribute-based access control for multiauthority cloud storage. *IEEE Systems Journal*, *12*(2), 1731–1742. doi:10.1109/JSYST.2016.2633559

Xue, Y., Hong, J., Li, W., Xue, K., & Hong, P. (2016). LABAC: a location-aware attribute-based access control scheme for cloud storage. In *2016 IEEE Global Communications Conference*. IEEE. doi:10.1109/GLOCOM.2016.7841945

Yamaguchi, T. F., Fujita, K., Ichimura, T., Hori, M., & Maddegedara, L. (2019). Acceleration of unstructured implicit low-order finite-element earthquake simulation using OpenACC on Pascal GPUs. *International Journal of High Performance Computing and Networking*, *13*(1), 3–18. doi:10.1504/IJHPCN.2019.097044

Yang, K., Liu, Z., Jia, X., & Shen, X. (2016). Time-domain attribute-based access control for cloud- based video content sharing: A cryptographic approach. *IEEE Transactions on Multimedia*, *18*(5), 940–950. doi:10.1109/TMM.2016.2535728

Yin, H., Zhao, Q., Xu, D., Chen, X., Chang, Y., Yue, H., & Zhao, N. (2019). 1.25 Gbits/s-message experimental transmission utilising chaos-based fibre-optic secure communications over 143 km. *International Journal of High Performance Computing and Networking*, *14*(1), 42–51. doi:10.1504/IJHPCN.2019.099738

Zhang, X. L., He, X. Y., Yu, F. M., Liu, L. X., Zhang, H. X., & Li, Z. L. (2019). Distributed and personalised social network privacy protection. *International Journal of High Performance Computing and Networking*, *13*(2), 153–163. doi:10.1504/IJHPCN.2019.097506

Zhang, Z., Han, L., Li, C., & Wang, J. (2016). A novel attribute-based access control model for multimedia social networks. *Neural Network World*, *26*(6), 543–557. doi:10.14311/NNW.2016.26.031

Zheng, H., He, J., Zhang, Y., Wu, J., & Ji, Z. (2019). A mathematical model for intimacy-based security protection in social network without violation of privacy. *International Journal of High Performance Computing and Networking*, *15*(3-4), 121–132. doi:10.1504/IJHPCN.2019.106084

Lanfang Zhang received the B.E. from College of International Education at Henan University of Science & Technology in 2016, and received the Master degree from College of Information Engineering, and Henan International Joint Laboratory of Cyberspace Security Applications, Henan University of Science & Technology, in 2020. She is presently teaching assistant at Henan University of Science & Technology. Her research interests include social network security and access control, social computing and social intelligence.

Zhiyong Zhang received his master's degree and Ph.D. in Computer Science from Dalian University of Technology and Xidian University, P. R. China, respectively. He was ever post-doctoral fellowship at School of Management, Xi'an Jiaotong University, China. Nowadays, he is a full-time Henan Province Distinguished Professor, Director of Henan International Joint Laboratory of Cyberspace Security Applications, and Vice-Dean of College of Information Engineering, Henan University of Science & Technology, China. He is also a visiting professor of Computer Science Department of Iowa State University. His research interests include cyber security and computing, social big data, multimedia content security. Recent years, he has published over 120 scientific papers and edited 6 books in the above research fields, and also holds 12 authorized patents. He is Chair of IEEE MMTC DRMIG, IEEE Systems, Man, and Cybernetics Society Technical Committee on Soft Computing, World Federation on Soft Computing Young Researchers Committee, Committeeman of China National Audio, Video, Multimedia System and Device Standardization Technologies Committee. And also, he is editorial board member and associate editor of Multimedia Tools and Applications (Springer), Human-centric Computing and Information Sciences (Springer), IEEE Access (IEEE), Neural Network World, EURASIP Journal on Information Security (Springer), leading guest editor or co-guest Editor of Applied Soft Computing (Elsevier), Computer Journal (Oxford) and Future Generation Computer Systems (Elsevier). And also, he is Chair/Co-Chair and TPC Member for numerous international conferences/ workshops on digital rights management and cloud computing security.

Ting Zhao received the B.E. from the College of Taiyuan University in 2018. She is currently pursuing master's degree with Henan International Joint Laboratory of Cyberspace Security Applications, Henan University of Science & Technology, Luoyang, China. Her research interests include cloud storage security.