IJERMT

International Journal Of Engineering Research & Management Technology

ISSN: 2348-4039

July- 2014 Volume 1, Issue-4

Email: editor@ijermt.org www.ijermt.org

Collaborative Authorization Framework for Security and Privacy in Social Networks

G.Satheesh
Assistant.Professor
Department of CSE
SVCET Chittoor A.P.

SMD.Mainuddin
Persuing M.Tech CSE
SVCET Chittoor A.P.

ABSTRACT—
Online social networks have explosive growth in recent years and become a default daily portal for some millions of Internet users. These Online Social Networks are attractive means for digital social interactions and information sharing, but also raise a security and privacy issues. While Social Networks permit users to restrict permission to shared data, they currently do not provide any special way to privacy concerns over data associated with collaborative users. To overcome these security and privacy issues, we have seen an approach to have the protection of shared data associated with multiple users in Online Social Networks. We formulated an access control model to capture the essence of collaborative authorization requirements. In addition to this in our paper the main frame work of translation module the Answer Set Programming (ASP) have added Infinitiary propositional formulas to it so that the properties of these programs can be more precisely characterized. By this, the features of the collaborative authorization frame work will effectively work. Nothing can be maintained secrecy in social networks

Key words: Social Networks, Collaborative Authorization Framework, and Answer set Programming (ASP)

1. INRODUCTION

Social networks play a key role in today's communication. Social networks like Face book, Whatsapp, Wechat etc. Each & every social network has different security measures, rules & regulations and policies. In face book if a user wants to share personal video to his friend's timeline, if he share that personal video to his friend's timeline it is publicly available in social networks. And every one can watch it even if he shares only with his friends if his friend likes it then it will appear publicly now anybody can watch it and any one can watch & like it .So here privacy & security will not present . In user's time line there is no protection for cover photos which will appear by opening of user's profile page.

In this paper, we formulated a systematic solution to facilitate collaborative authorization frame work for shared data in social networks. We begin by examining how the lack of multiparty access control (MPAC) for data sharing in SNs can determine the protection of user data. Some typical data sharing patterns with respect to collaborative authorization in SNs are also identified. Based on these sharing patterns, an MPAC model is formulated to capture the core features of multiparty authorization requirements that have not been accommodated so far by existing access control systems and models for SNs[4], [5]. Our model also contains a multiparty policy specification scheme. Meanwhile, since conflicts are inevitable in multiparty authorization enforcement, a voting mechanism is further provided to deal with authorization and privacy conflicts in our model. In addition to the systematic solution we added extended features to the ASP programming by this the collaborative authorization frame work will work effectively.

Social networks (SNs) such as Face book, Whatsapp and We chat are inherently designed to enable people to share personal and public information and make social connections with friends, co-workers, colleagues, family and even with strangers. In recent years, we have seen explosive growth in the application of SNs. For example, Face book, one of representative widely using social network sites, claims that it has more than 1000 million active user's and over 50 billion pieces of content (news, stories, friends groups, games, adds, television channel links, online marketing links etc.) shared every week[1]. To protect user data, access control has become a main feature of SNs [2], [3].

A typical Social Network provides each user with a virtual space containing profile information, user's friends list, personal information, and user uploaded photo's will be present such as timeline in Face book, where users friends can post any content and leave status messages. A user profile usually includes information with respect to the user's birthday, gender, interests, relationship, education & working details, and contact information. In addition, users can upload content into their own or other's timeline but also they can tag other user's who appear in the content. Each tag is an explicit reference that connects to the user's timeline. For the user data protection, current SNs indirectly require users to be system and policy administrators for regulating their data, where users can restrict data sharing to a specific set of trusted users. SNs often use user relationship and group will be divided close friends & normal friends to differentiate between trusted and untrusted users. For example, in Face book, users can allow friends (F), friends of friends(FOF), relationship, and public to access their data, depending on their personal authorization and privacy requirements.

2. LITERATURE SURVEY

Protection of privacy data in social networks is still a relatively new research area. Several access control models for SNs have been introduced, among those concepts we can discuss some important concepts.

2.1. RULE BASED ACCESS CONTROL FOR SECURITY AND PRIVACY IN ONLINE SOCIAL NETWORKS

In the era of Internet technologies, social networking websites has witnessed thriving popularity. Computer mediated communication has changed the rules of social interaction and communication. Most social networking sites like Face book, Wechat, whatsapp etc. Facilitates user's with the features like online interactions, sharing of information and connecting new relationships etc. Online interaction and sharing of personal information in social networking sites has raised new privacy concerns. So, it requires an exploratory insight into user's behavioural intention to share information. This research aims to develop a research model, with security and privacy concerns conceptualized as an antecedent of trust in social networking site and moderator of information sharing. The study aims to understand the impact of security, trust and privacy concerns on the willingness of sharing information in social networking sites. Using an online questionnaire, empirical data were collected from 250 Face book user's of different age group over the time period of 4 months. Reliability analysis, confirmatory factor analysis, structure equation modelling is used to validate the proposed research framework. This empirical study, based on an established theoretical foundation, will help the research community to gain a deeper understanding of the impacts of privacy concern in the context of Facebook. Enforcing Access Control in Web-based Social Networks In this paper, we propose an access control mechanism for Web-based Social Networks, which adopts a rule-based[5] approach for specifying access policies on the resources owned by network participants, and where authorized users are denoted in terms of the type, depth, and trust level of the relationships existing between nodes in the network. Differently from traditional access control systems, our mechanism makes use of a semi-decentralized architecture, where access control enforcement is carried out client-side. Access to a resource is granted when the requestor is able to demonstrate of being authorized to do that, by providing a proof. In the paper, besides illustrating the main notions on which our access control model relies, we present all the protocols underlying our system and a performance study of the implemented prototype.

A. PROPOSED HYPOTHESIS

The proposed hypothesis aims to find impact of privacy, security, and trust on the willingness to share information in social networking site. According to proposed hypothesis; perceived security, perceived privacy and perceived trust are the factors that influence user's willingness to share information in social networking sites. Thus the hypotheses are summarized in table.1.

The constructs used in our hypothesized model are defined in table.2.

Table.1 Research Hypothesis

H#	Hypothesis
H1	Perceived security is positively related to perceived trust with in social networking sites
H2	Perceived privacy is positively related to perceived trust with in social networking sites
H3	Perceived security is positively related to information sharing in social networking sites
H4	Perceived privacy is positively related to information sharing in social networking sites
H5	Perceived trust is positively related to information sharing in social networking sites

Table.2 Construct Definitions

Construct	Definition
Perceived privacy	Extent to which an individual have Control over his information flow and protection of his profile privacy.
Perceived trust	And individual belief in the ability of social networking site that revealing info and performing any task is risk free.
Perceived security	An individual belief that using social networking site over internet is risk free.
Information sharing	An individual belief that they will continue to share information over social networking site with regard to privacy concerns

2.2. A COLLABORATIVE ACCESS CONTROL FOR PRIVACY PROTECTION IN ONLINE SOCIAL NETWORKS

With the wide use of online social networks (OSNs), the problem of data privacy has attracted much attention. Several approaches have been proposed to address this issue. One of privacy management approaches for OSN leverages a key management technique to enable a user to simply post encrypted contents so that only users who can satisfy the associate security policy can derive the key to access the data. How- ever, the key management policies of existing schemes may grant access to unauthorized users and cannot efficiently determine authorized users. In this paper, we propose a collaborative framework [4] which enforces access control for OSN through an innovative key management focused on communities. This framework introduces a community key management based on a new group-oriented convergence cryptosystem, as well as provides efficient privacy preservation needed in a private OSN. To prove the feasibility of our approach, we also discuss a proof-of-concept implementation of our framework. Experimental results show that our construction can achieve the identified design goals for OSNs with the acceptable performance.

A. CONTRIBUTIONS

To meet the privacy needs of OSN, we present a solution. Which fulfils above-mentioned requirements. Our collaborative framework can provide flexible, efficient privacy protections needed in a private OSN without the intervention of a system manager. We briefly summarize the contributions of our work in this paper.

1. We propose a system architecture for a private OSN. In this architecture community creators can collaborate to manage and maintain their communities. There is no need for a centralized management server to build PKC/PK1 for key exchange and to monitor the behaviour of all users;
2. We provide a community key management method for our architecture based on a new group-oriented convergence cryptosystem (GCC). This method leverages the following properties: the community is built on convergence of some users' private keys, the upload and download of resources provide the authentication and integrity checking, as well as there exist efficient mechanism for access permission delegation and sophisticated revocation.

3. PROBLEM DEFINITION

The literature on privacy protection in social networks reports the uses of access control models cannot give security up to the mark by this literature we need to find some more models and mechanisms to protect the data in SNs. Till now the implemented access control models are used upto the mark now the privacy issues are more than obviously the solutions also more.

3.1. EXISTING METHOD

The existing work could model and analyze access control requirements with respect to collaborative authorization management of shared data in social networks. The need of joint management for data sharing, especially photo sharing, in SNs has been recognized by the recent work provided a solution for collective privacy management in SNs. Their work considered access control policies of a content that is co-owned by multiple users in an SN, such that each co-owner may separately specify her/his own privacy preference for the shared content.

Although SNs currently provide simple access control mechanisms allowing users to govern access to information contained in their own timeline, users, unfortunately, have no control over data residing outside their timeline. For instance, if a user posts a comment in a friend's timeline, he/she cannot specify which users can view the comment.

4. PROPOSED METHOD

And in this paper we are adding extendable formulas to the translation program ASP called GRINGO. Gringo is the name of the input language of the grounder GRINGO, which is used as the front end in many answer set programming (ASP) systems. After implementing these infinitiary propositional formulas in logical representation and analysis of collaborative authorization framework access control. The translation module will work effectively. We propose to approach the problem of defining the semantics, by translating them into the language of infinitiary propositional formulas. Thus semantics allow us to study equivalent transformations of GRINGO programs using natural deduction in infinitiary propositional logic, so that the properties of these programs can be more precisely characterized.

4.1 MODULE DESCRIPTION

Number of modules after careful analysis the system has been identified to have the following modules.

1. Owner
2. Contributor
3. Stakeholder
4. Disseminator
5. MPAC

1. OWNER - In Owner step let *d be* a data item in the timeline m of a user *u* in the social network. The user *u* is called the owner of *d*. The user *u* is called the contributor of *d*. We specifically analyze three scenarios—profile sharing, relationship sharing and content sharing—to understand the risks posted by the lack of collaborative control in OSNs. In this the owner and the disseminator can specify access control policies to restrict the sharing of profile attributes. Thus, it enables the owner to discover potential malicious activities in collaborative control. The detection of collusion behaviours in collaborative systems has been addressed by the recent work.

2. CONTRIBUTOR - In Contributor step let *d* be a data item published by a user *u* in someone else's timeline in the social network. The contributor publishes content to other's timeline and the content may also have multiple stakeholders (e.g., tagged users). The memory space for the user will be allotted according to user request for content sharing. A shared content is published by a contributor

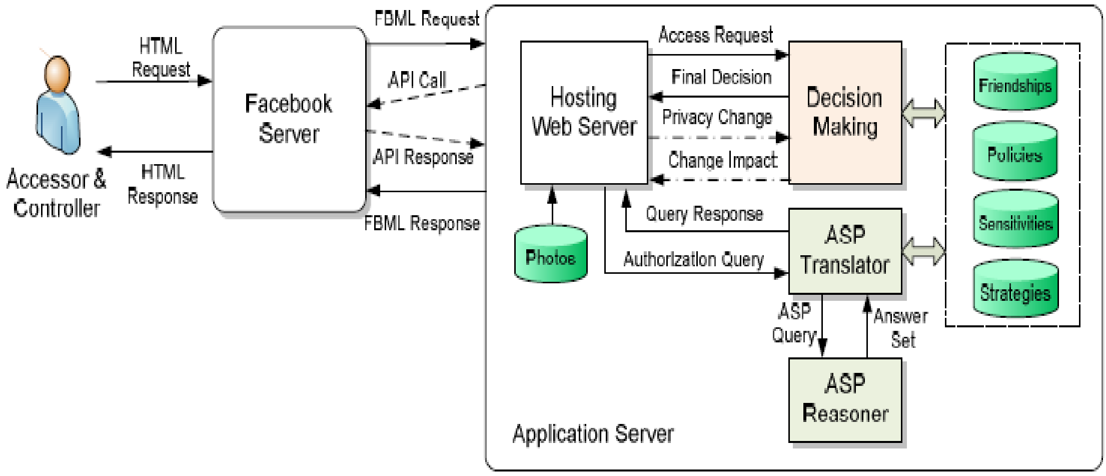
3. STAKEHOLDER - In stakeholder step let *d* be a data item in the timeline of a user in the social network. Let *T* be the set of tagged users associated with *d*. A user *u* is called a stakeholder of *d*, if *u 2 T* who has a relationship with another user called stakeholder, shares the relationship with an accessor. In this scenario, authorization requirements from both the owner and the stakeholder should be considered. Otherwise, the stakeholder's privacy concern may be violated. A shared content has multiple stakeholders.

4. DISSEMINATOR - In disseminator step let *d* be a data item shared by a user *u* from someone else's timeline to his/her timeline in the social network. The user *u* is called a disseminator of *d*. A content sharing pattern where the sharing starts with an originator (owner or contributor who uploads the content) publishing the content, and then a disseminator views and shares the content. All access control policies defined by associated users should be enforced to regulate access of the content in disseminator's timeline. For a more complicated case, the disseminated content may be further re-disseminated by disseminator's friends, where effective access control mechanisms should be applied in each procedure to regulate sharing behaviours. Especially, regardless of how many steps the content has been redisseminated, the original access control policies should be always enforced to protect further dissemination of the content.

5. MPAC- Multiparty access control (MPAC) is used to prove our access control step is valid. To enable a collaborative authorization management of data sharing in SNs, it is essential for multiparty access control policies to be in place to regulate access over shared data, representing authorization requirements from multiple associated users. Our policy specification scheme is built upon the MPAC step.

5. EXPERIMENT EVALUATION

In the fig.1 you notice that the ASP Translator and ASP Reasoner are present in application server side here we are proposing the GRINGO programs. And in this ASP Translator and ASP Reasoner we are adding extendable formulas called GRINGO. Gringo is the name of the input language of the grounder GRINGO, which is used as the front end in many answer set programming (ASP) systems.



After implementing these Infinitiary propositional formulas in logical representation and analysis of collaborative authorization framework access control. The translation module will work effectively. We propose to approach the problem of defining the semantics, by translating them into the language of infinitiary propositional formulas. Thus semantics allow us to study equivalent transformations of

GRINGO programs using natural deduction in infinitiary propositional logic, so that the properties of these programs can be more precisely characterized.

$$P(y) \leftarrow count\{x,y:q(x,y)\} \geq 1 (1)$$

can be represented by the sentence

$$\forall y\ (\exists x Q\ (x,y) \rightarrow P\ (y))$$

5.1 USER STUDY OF MCONTROLLER

Table.3 USER STUDY OF MCONTROLLER

	Facebook		Mcontroller	
Metric	**Avg**	**UB on 95% CI**	**Avg**	**LB on 95% CI**
Likability	**0.20**	**0.25**	**0.83**	**0.80**
Simplicity	**0.38**	**0.44**	**0.72**	**0.64**
Control	**0.20**	**0.25**	**0.83**	**0.80**

UB- upper bound, LB-lower bound, CI-confidence interval

For evaluation purposes, questions were split into three areas: likability, simplicity, and control. Likability is a measure of a user's satisfaction with a system. Simplicity is a measure how intuitive and useful system. Control is a measure of the user's perceived control of their personal data (e.g., "If Face book implemented controls like MController's to control photo privacy, my photos would be better protected"). Questions were either True/False or measured on a 5-point Likert scale, and all responses were scaled from 0 to 1 for numerical analysis. In the measurement, a higher number indicates a positive perception or opinion of the system while a lower number indicates a negative one. To analyze the average user perception of the system, we used a 95percent confidence interval for the users' answers. This assumes the population to be mostly normal.

6. CONCLUSION

In this paper, we have proposed a novel solution for collaborative management of shared data in SNs. A multiparty access control model was formulated, along with a multiparty policy specification scheme and corresponding policy evaluation mechanism. In addition, we have introduced an approach for ASP Translator and reasoner in our proposed model. A proof-of-concept implementation of our solution called MController has been discussed as well, followed by the usability study and system evaluation of our method. As part of future work, we are planning to investigate more comprehensive privacy conflict resolution approach, and analysis services for collaborative management of shared data in SNs. Also, we would explore more criteria to evaluate the features of our proposed MPAC model. For example, one of our recent work has evaluated the effectiveness of the MPAC conflict resolution approach based on the tradeoffs of privacy risk and sharing loss. In addition, users may be involved in the control of a larger number of shared photos and the configurations of the privacy preferences may become time-consuming and tedious tasks. Therefore, we would study inference-based techniques for automatically configure privacy preferences in MPAC. Besides, we plan to systematically integrate the notion of trust and reputation into our MPAC model and investigate a comprehensive solution to cope with collusion attacks for providing a robust MPAC service in SNs.

7. ACKNOWLEDGEMENT

SMD.Mainddin would like to thank Sri Venkateswara College of Engineering And Technology, Head of The Department Dr.J.Janet and guide G.Satheesh, Assistant professor for their help and support.

REFERENCES

1. Face book Privacy, http://www.facebook.com/policy.php/, 2013
2. Face book Statistics, http://www.facebook.com /press / info.php?statistics, 2013
3. Google+ Privacy Policy, http://www.google.com/intl/en/+/policy/, 2013
4. B. Carminati and E. Ferrari, "Collaborative Access Control in Online Social Networks," Proc. Seventh Int'l Conf. Collaborative Computing: Networking, Applications and Worksharing Collaborative-com), pp. 231-240, 2011.
5. B. Carminati and E. Ferrari, and A. Perego, "Rule-Based Access Control fro Social Networks," Proc. Int'l Conf. On the move to Meaningful Internet Systems, pp. 1734-1744, 2006.
6. P. Fong, "Relationship-Based Access Control: Protection Model and Policy Language," Proc. First ACM Conf. Data and Application Security and Privacy,pp. 191-202, 2011.
7. H. Hu and G. Ahn, "Multiparty Authorization Framework for Data Sharing in Online Social Networks," Proc. 25th Ann. IFIP WG 11.3 Conf. Data and Application Security and Privacy, pp. 29-43, 2011.