www.ijiarec.com

ISSN:2348-2079

Volume-7 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Scalable access control for privacy-aware media sharing

Mrs.Vanitha[1], S.Mahesawaran[2], M.Manjula Devi[2], P.Manoranjitham[2]

[1]Assistant Professor, Department of Computer Science and Engineering, Nandha Engineering College

[2]UG Students Department of Computer Science and Engineering, Nandha Engineering College

ABSTRACT

The prevalence of social networks has created it easier than ever for users to share their photos, videos and different media content with anybody from anyplace. However, the straight forward access of user-generated media content additionally brings concerning privacy considerations. Traditional access management mechanisms, wherever one access policy is created for a selected piece of content, cannot satisfy the user privacy needs in large-scale media sharing systems.. On one hand, it conforms to the principle of social networks in info propagation. On the opposite hand, it accords with the varied and sophisticated social relationship among social network users. In this paper, we have a tendency to propose a ascendible media access management (SMAC) system to alter such a configuration in a very secure and economical manner. The projected SMAC system is scepter by the ascendible ciphertext policy attribute-based secret writing (SCP-ABE) algorithmic rule still as a comprehensive key management theme. We provide formal security proof to prove the protection of the projected SMAC system Additionally, we have a tendency to conduct intensive experiments on mobile devices to demonstrate its potency [1, 2].

Index terms: Social Media Sharing, Privacy, Access Control, SCP-ABE, Scalable Media Format

INTRODUCTION

The prevalence of social networks has boosted the advancement of a variety of user generated content (UGC) such as texts, photos, and videos. The popularity and the easy access of UGC brings about new opportunities for numerous applications such as personal branding and commercial advertising. For example, photographers can utilize Instagram and Flickr to promote their works. Similarly, users can advertise products, ideas, and themselves by creating YouTube channels. However, UGC sharing also results in privacy concerns. One of the primary privacy concerns is content repurposing by third parties.

For example, the content shared on social networks can be plagiarized by others and served for their own profitable purpose Additionally, displaying informative media content such as photos and videos on the social networks can easily disclose sensitive user information, such as friendships, hobbies, and footprints, to untrusted ones. With the advancement of image/video processing and artificial intelligence techniques that might uncover more personal information, the privacy concerns caused by UGC sharing will become critical. The root cause of the privacy issues in UGC sharing is that users have little control on the information propagation in social networks, i.e. who will be viewing their shared content. Although users can usually enable or disable other users to access their shared content by configuring privacy settings on social networks, they cannot prevent social network servers from

Author for correspondence:
Department of Computer Science and Engineering, Nandha Engineering College, Erode, Tamilnadu, India

leaking their content to third parties without their authorization.

In this paper, we propose a scalable media access control (SMAC) system to achieve this goal. In the proposed system, a media stream is encoded into multiple levels of perceptual quality by exploiting techniques. In the SMAC system, sacrificing the breath of media content propagation is not the only choice for user privacy preservation.

Personal use is allowable.

For example, a content owner can enable every user in the media sharing system to access the low quality version of the content, but only allow the trusted ones to view a high quality version. The rationality of the mechanism relies on that the low-quality media content is less commonly used in re-purposing and is more robust in resisting analysis based attacks than the high-quality media content. Such a mechanism is especially expected when the users do not need a very restricted access policy on their shared media content. Additionally, the SMAC system is able to support arbitrary levels of trust relationship by configuring the same number of access policies efficiently.

This way, we can ensure that the content with a specific quality is propagated along the corresponding trusted chain. Developing the SMAC system is faced with two non-trivial challenges: 1) how to securely enforce multiple access policies for a scalable media stream; 2) how to reliably authenticate the access privileges of content consumers and manage their dynamics [3],[4].

In scalable media format, a media stream is encoded into a base layer providing the basic quality and multiple enhancement layers enhancing the quality. The quality can be enhanced from multiple dimensions such as resolution, SNR, and frame rate. Such kind of multi-dimensional scalability is a special characteristic of media content. As an illustration, we show the data structure of a 2-by-3-by-2 scalable media stream.

The consumer can enjoy higher SNR and resolution. Under such a data structure, the media consumption experience can be effectively controlled by adjusting the transmitted media layers upon sharing.

Developing the SMAC system is faced with two non-trivial challenges: 1) how to securely enforce multiple access policies for a scalable media stream; 2) how to reliably authenticate the access privileges of content consumers and manage their dynamics. To tackle these challenges, we first propose a scalable cipher text policy attribute-based encryption (SCP-ABE) algorithm that can securely encrypt a multi-dimensional scalable media stream [12].

Under a set of social attribute-based access policies, the media stream can be decoded into media content with various levels of quality from multiple dimen-sions. Thus a content consumer whose social attributes satisfy the access policy will obtain the right access keys to decrypt the media stream, and decode and view the content with a specific quality. If a consumer's attributes match more than one access policy of the media stream, the individual will enjoy a higher access privilege and a higher viewing quality of the content. Furthermore, we propose a comprehensive key management scheme to handle the access key distribution and revocation. It is able to reliably authenticate the attributes of consumers, and distribute and revoke their corresponding access keys. In addition, the proposed scheme shifts most of the key management cost from the content distributer side to the more powerful social network server side. In this way, the privacy preservation cost on the distributor side does not increase with the number of content consumers but only depends on the number of shared contents. Through formal security analysis, we prove the security and reliability of the SMAC system. Furthermore, we conduct practical experiments on mobile devices to demonstrate its efficiency.

To summarize, we make the following contributions.

We present the first access control scheme that protects user privacy in large-scale media sharing systems, sat-isfying two essential user requirements, i.e., widespread content propagation and multiple-level access privileges.

We propose a SCP-ABE algorithm that is able to securely enforce multiple access policies on multi-dimensional scalable media streams.

We propose a comprehensive key management scheme that facilitates the reliable and efficient access privilege authorization and revocation.

This paper is organized as follows. In Section II, we intro-duce the background and the related work. In Section III, we present the overview of the SMAC system. We then introduce the implementation details of SMAC from two aspects, i.e., how to enforce multiple access policies for the scalable media data, and how to authorize and revoke the access privileges of media content consumers, in Section IV and Section V, respectively. ,we evaluate the performance of the proposed system in terms of security and efficiency. authorities among the previous, whereas every owner solely must manage the keys of tiny low vary of users in her personal domain [5],[6].

Existing system

In the Existing system brings new and challenging securitythreats.Users outsourced data are separate administrative entities,data outsourcing is actually relinquishing user's ultimatecontrol over the fate of their data.As a result, the correctness of the data is being put at risk duet the following reasons.

Drawbacks

- Facing broad range of both internal and external threats for data integrity.
- For the benefits of their own, there do exist various motivations for cloud service providers to behave unfaithfully towards the cloud users regarding the status of their outsource data[7].

Proposed system

- We motivate the public system of data storage security andprovide a privacy aware media sharing.Outsourced data
- without learning knowledge on the datacontent. To the best of our knowledge, we achieve the following.

ADVANTAGES

Support scalable access control for privacy aware mediasharing. In our scheme achieves batch where multiple delegated, We prove the security and justify the performance of our proposed schemes through concrete experiments and comparisons with the state-of-the-art[8].

INPUT DESIGN

Input design is the process of converting user-originated inputs to a computer understandable format Input design is one of the most expensive phases of the operation of computerized system and is often the major problem of a system. A large number of problems with a system can usually be tracked backs to fault input design and method. Every moment of input design should be analyzed and designed with utmost care.

The system takes input from the users, processes it and produces an output. Input design is link that ties the information system into the world of its users. The system should be user-friendly to gain appropriate information to the user. The decisions made during the input design are

- To provide cost effective method of input.
- To achieve the highest possible level of accuracy.
- To ensure that the input is understand by the user.

System analysis decide the following input design details like, what data to input, what medium to use, how the data should be arranged or coded, data items and transactions needing validations to detect errors and at last the dialogue to guide user in providing input [11],[13].

Input data of a system may not be necessarily is raw data captured in the system from scratch. These can also be the output of another system or subsystem.

Testing is vital to the success of the system. System testing makes a logical assumption that if all parts of the system are correct, the goal will be successfully achieved. In the testing process we test the actual system in an organization and gather errors from the new system operates in full efficiency as stated. System testing is the stage of implementation, which is aimed to ensuring that the system works accurately and efficiently.

In the testing process we test the actual system in an organization and gather errors from the new system and take initiatives to correct the same. All

the front-end and back-end connectivity are tested to be sure that the new system operates in full efficiency as stated. System testing is the stage of implementation, which is aimed at ensuring that the system works accurately and efficiently.

- Inadequate testing or non-testing leads to errors, that may appear few months later. This will create two problems
- Time delay between the cause and appearance of the problem.
- The effect of the system errors on files and records within the system.
- The purpose of the system testing is to consider all the likely variations to which it will be suggested and push the system to its limits [9],[10].

OUTPUT DESIGN

Output design generally refers to the results and information that are generated by the system for many end-users; output is the main reason for developing the system and the basis on which they evaluate the usefulness of the application. The output is designed in such a way that it is attractive, convenient and informative. Forms are designed in various features, which make the console output more pleasing. As the outputs are the most important sources of information to the users, better design should improve the system's relationships with user and also will help in decision-making. Form design elaborates the way output is presented and the layout available for capturing information. .All records from various databases with same table names are retrieved.

In this way, the privacy preservation cost on the distributor side does not increase with the number of content consumers but only depends on the number of shared contents. Through formal security analysis, we prove the security and reliability of the SMAC system. Furthermore, we conduct practical experiments on mobile devices to demonstrate its efficiency.

Input data of a system may not be necessarily is raw data captured in the system from scratch. These can also be the output of another system or subsystem.

Testing is vital to the success of the system. System testing makes a logical assumption that if all parts of the system are correct, the goal will be successfully achieved. In the testing

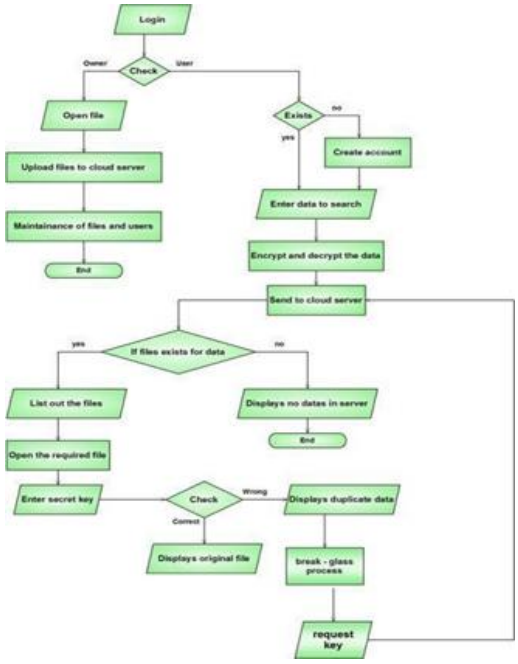

Figure 1: knowledge multidimensional language

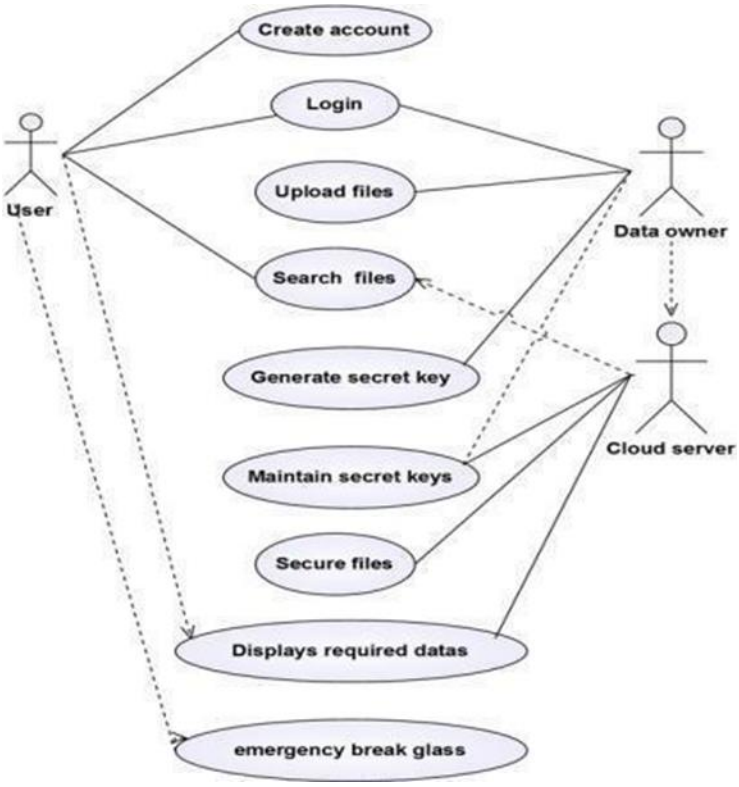

Figure 2: Use Case Diagram

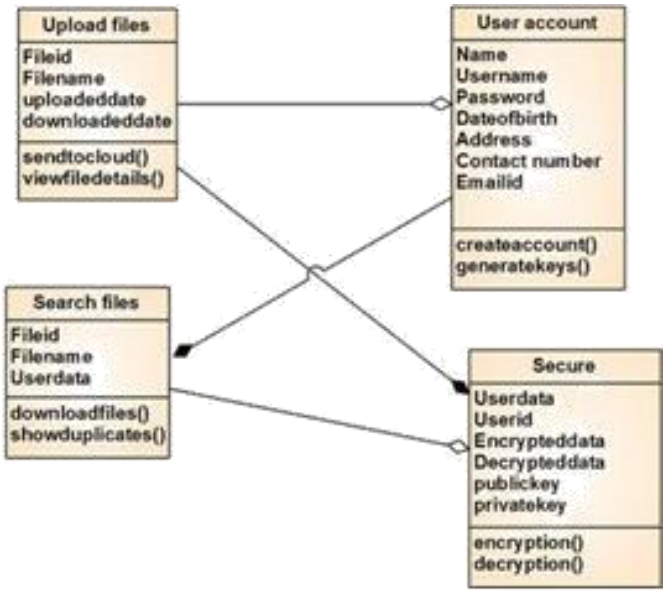

Figure 3: Class Diagram

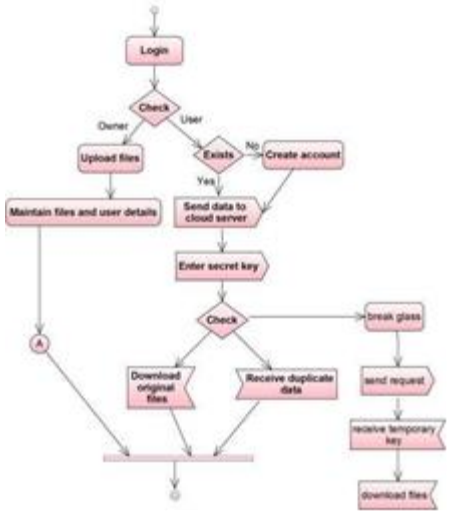

Figure 4: Activity Diagram

literature survey

The practicability of the project is analyzed during this section and business proposal is place forth with a awfully general arrange for the project and a few price estimates. throughout system analysis the practicability study of the planned system is to be allotted. this can be to confirm that the planned system isn't a burden to the corporate. For practicability analysis, some understanding of the main necessities for the system is important [15].

Three key issues concerned within the practicability analysis area unit

- Economical practicability
- Technical practicability
- Social practicability

Economical feasibleness

This study is dole out to envision the economic impact that the system can wear the organization. the number of fund that the corporate will pour into the analysis and development of the system is restricted. The expenditures should be even. So the developed system moreover among the budget and this was achieved as a result of most of the technologies used area unit freely on the market. solely the made-to-order merchandise had to be purchased [14].

Technical feasibleness

This study is dole out to envision the technical feasibleness, that is, the technical needs of the system. Any system developed should not have a high demand on the on the market technical resources. this can result in high demands on the on the market technical resources. this can result in high demands being placed on the shopper. The developed system should have a modest demand, as solely token or null changes area unit needed for implementing this technique [14].

Social feasibleness

The facet of study is to visualize the extent of acceptance of the system by the user. This includes the method of coaching the user to use the system expeditiously. The user should not feel vulnerable by the system, instead should settle for it as a necessity. the extent of acceptance by the users only depends on the strategies that are used to teach the user regarding the system and to create him acquainted with it. His level of confidence should be raised in order that he's additionally ready to create some constructive criticism,that is welcome, as he's the ultimate user of the system.

The expenditures should be even. So the developed system moreover among the budget

and this was achieved as a result of most of the technologies used area unit freely on the market [14].

MODULES

- Personal Tweet module
- Permission allot module
- Encrypted module
- Access module

Personal tweet module

- The registered user can login these module.
- Twitter home page suggests the social platform can be used to connect with your friends-and other fascinating people.
- Get in the moment updates on the things that interest you.

Encrypted module description

- The easy access of user generated media content also brings about privacy concern.
- The proposed system contains cyber text policy attribute based encryption algorithm.

Permission allot module discription

- The registered user can login these module.
- Twitter home page suggests the social platform can be used to connect with your friends-and other fascinating people.
- Get in the moment updates on the things that interest you.

Access module description

- The shared media can access by key given by the sender.
- The key received by them through email.
- They can unlock the media using the key .

RESULTS & CONCLUSION

In this paper, we have presented SMAC, the first access control scheme that protects user privacy in large-scale media sharing systems and satisfies two essential user requirements, i.e., widespread content propagation and multiple-level access privileges. In particular, we first propose a SCP-ABE algorithm to enable secure enforcement of multiple access policies on the multi-dimensional scalable media streams. In addition, we propose a comprehensive key management scheme to facilitate the reliable and efficient access privilege authorization and revocation. We have proved the security and reliability of the SMAC system. We also demonstrated its efficiency on mobile devices through experiments. We believe these features of the SMAC system will contribute to the wide adoption of privacy preservation in large-scale social networks. For the future work, we will extend the SMAC system to support media sharing across multiple social networks to accord with the trending cloud-based services [15],[16].

REFERENCES

[1]. A Framework for Composition and Enforcement Privacy-Aware and Context-Driven Authorization Mechanism for Multimedia Big Data," IEEE Transactions on Multimedia, 17, 2015, 1484-1494.
[2]. Bethencourt, J.; Sahai, A.; Waters, B., Ciphertext-Policy Attribute-Based Encryption," IEEE Symposium on Security and Privacy, 2007, 321-334,.
[3]. B.Preneel,“Cryptographic hash functions," European Trans. Telecom., 5 (1994), pp. 431-448, 1994.
[4]. C. Zhang, J. Sun, X. Zhu and Y. Fang, “Privacy and security for online social networks: challenges and opportunities," IEEE Network, 24, 2010, 13-18.
[5]. Crampton, J.; Daud, R.; Martin, K. M., “Constructing Key Allignment Schemes from Chain Partitions," IFIP WG 11.3 working conf. on Data and applications security and privacy, 2010.
[6]. D. Hankerson, A. Menezes, S. Vanstone, “Guide to Elliptic Curve Cryptography," Springer-Verlag New York, Inc. 2004. ISBN 0-387-95273-X.

[7]. D. M. Dumbere and N. J. Janwe, “Video encryption using AES algorithm," Second International Conference on Current Trends In Engi-neering and Technology (ICCTET), 2014, 332-337.
[8]. F. Dufaux and T. Ebrahimi, “Scrambling for Privacy Protection in Video Surveillance Systems," IEEE Transactions on Circuits and Systems for Video Technology, 18(8), 2008, 1168-1174.
[9]. Jun Zhou et al, “4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks," Inf. Sci. 314, 2015, 255-276.
[10]. J. Zhou, X. Dong, Z. Cao and A. V. Vasilakos, “Secure and Privacy Preserving Protocol for Cloud-Based Vehicular DTNs," IEEE Trans. Information Forensics and Security, 10(6), 2015, 1299-1314.
[11]. K. G. Paterson, “ID-based signatures from pairings on elliptic curves," Electronics Letters, 38(18), 2002, 1025-1026.
[12]. M. R. Rahimi, J. Ren, C. H. Liu, A. V. Vasilakos, N. Venkatasubrama-nian, “Mobile Cloud Computing: A Survey, State of Art and Future Direc-tions," Mobile Netw Appl 19, 2014, 133. https://doi.org/10.1007/s11036-013-0477-4
[13]. M. Ali et al., “SeDaSC: Secure Data Sharing in Clouds," IEEE Systems Journal, 11(2), 2017, 395-404.
[14]. M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, “Deep Learning with Differential Privacy," CCS, 2016, 308-318.
[15]. M. Fire, R. Goldschmidt and Y. Elovici, “Online Social Networks: Threats and Solutions," IEEE Communications 2014.