Developing Multimedia Services in Mobile Social Networks from Security and Privacy Perspectives

D Murugeswari*[1], *Assistant Professor
Department of Computer Science, Thassim Beevi Abdul Kader College for Women, Kilakarai
Email: murugeswari2412@gmail.com
B Thillaieswari*[2], *Assistant Professor
Department of Computer Science, Thassim Beevi Abdul Kader College for Women, Kilakarai
Email: thillaikris@gmail.com

ABSTRACT

Multimedia services, smart phones and traditional online multimedia applications are enlarged to mobile users anywhere and anytime. However, the successful of multimedia services is now delayed by inherent security and privacy concerns. In this paper, we investigate the security and privacy issues of multimedia services by studying a newly emerging multimedia-oriented mobile social network (MMSN), which helps users, receive multimedia services not only from their online social communities but also from their social friends in their surrounding area. Particularly, we first describe the MMSN architecture, and recognize the unique security and privacy challenges. Then we investigate three MMSN applications: extract information, service estimation, and content sorting. For each application, we present the specific security and privacy problems with the corresponding threats. Finally, we suggest some future research directions in the MMSN.

Keywords: content sorting, encrypted content upload, extract information, range query predicate construction, service estimation

INTRODUCTION

Multimedia is gradually more becoming content driven and object-oriented, endorse applications with user collaboration in the current fashion. In 2014, in every minute of the day, 200,000 tweets are posted; 48 hours of videos are updated on Youtube with 3,800,000 video views; 785,000 pieces of contents are shared on Facebook; and 3.5 billion queries are conducted on Google per day. As the amount of multimedia services skyrockets, it is leading importance for users to not only share multimedia contents with each other but also receive the content of their interests. A mobile social network increased with heterogeneous wireless infrastructures and mobile devices, has become potential and popular platform to enable user relationship and information sharing. It can also help multimedia services by providing universal connections between service providers and users in a mobile environment.

The mobile social network is dramatically changing users' lifestyles, and promotes a value-added research area of the multimedia-oriented mobile social network. This newly emerging MMSN provides users with modern contents from a centralized server and local contents directly shared by their friends nearby. Specifically, users can directly select and download the multimedia contents in which they are interested from centralized servers via the Internet; local service providers such as stores could distribute local contents to mobile users in a distributed manner; and a group of users in one social community might separately form an prospect network and share personalized contents via peer to- peer communication. In spite of the promising features of multimedia services provided by the MMSN, there are many new challenges in the privacy and security aspects.

In an MMSN, personalized extract information is a distinctive multimedia service, but it may disclose a user's personal information to service providers. For example, Google could record a user's queries and analyze his/her preferences. Moreover, when users visit social networking sites with "Facebook Like" buttons and press the button, they disclose their preferences and personal information, such as location and identity, to the public. Furthermore, service evaluation is another multimedia application where users post their reviews or experiences about services they use. However, Sybil attackers could fake a large number of pseudonyms and gain unreasonably negative influence. These attackers would either purposely generate positive comments on their own services or arbitrarily produce negative reviews on other quality services. So, preserving privacy and oppose malicious attacks are critical research challenges that need to be addressed for an MMSN. In this paper, we define the MMSN architecture and identify some research issues related to privacy preservation, trust relationships, and malicious attacks. And also, we present three emerging MMSN applications: personalized extract information, service estimation, and content sorting. We examine the security and privacy problems in these applications, and present the corresponding threats. Finally, we present some possible research directions and conclude the paper.

2. MMSN ARCHITECTURE

In this section, we present various MMSN architecture and classify the entities with special message patterns. Then we classify the MMSN into different domains.

2.1 MMSN ARCHITECTURE

The MMSN, as shown in Fig. 1, is a virtual atmosphere composed of mobile users in a local area, local servers, and centralized servers.

Multimedia: Multimedia contents are fundamental to the MMSN, and vary in dissimilar applications. In general, multimedia can be global content, like online video, local content and personal contents including personal information and images. It may be small and large ranging from multiple contents, such as photos with contents image to videos and even movies.

Mobile Users: Mobile users with smart phones can moreover directly connect to the Internet via cellular / WiFi networks or communicate with adjacent users in the environs via Bluetooth/ near field communication (NFC) techniques. The communication patterns and modes are resolute by ecological conditions and application necessities. When users are searching the Internet contents such as You tube video, they force switch to Internet mode and directly access the intention servers to obtain the desirable contents. Users in the environs can directly swap their personal contents as well as local information and other multimedia contents with every other via Bluetooth. Mobile users not only are the content owners but also aim to query or acquire contents from others.

Local Server: The local server (LS) can offer local services, such as advertisements and service estimation of stores, to users in the vicinity. LSs are prepared with smart phones or devoted mobile local gateways, which broadcast their service information to nearest mobile users and gather user feedback or requests. The LS's communication procedures are storeroom-rich and fueled by sufficient power. The multimedia contents of LSs are essentially about local information including service description, local introduction and tips, advertisements, and so on.

Centralized Servers: Centralized servers (CSs), such as ISP and clouds, can provide federal services to mobile users due to the high capabilities of storage, communication, and computation of CSs.

2.2 MMSN DOMAINS

The MMSN can usually be divided into three domains: User-to-CS, User-to-LS, and User-to- User domains according to diverse communication patterns and multimedia contents.

User-to-CS Domain: In the User-to-CS domain, mobile users can bluntly connect with the CS via besides cellular networks with a purchased mobile information plan or WiFi access points, which are pervasively deployed in the built-up community and communal spots such as campuses and provisions. The communication alternative depends on the network infrastructures, and connections can be one-hop or multi hop. The contents communicated contained by the User-to-CS domain consist of a broad range of multimedia all over the world. Users can look around online multimedia contents like social media, photo collections, and movies, inquiry the enviable contents, and share their multimedia contents via the Internet.

User-to-LS Domain : In the User-to-LS domain, the LS acts as not only a temporary local server, which is equipped with the easy-to setup and low-cost local wireless gateway or router, but also a mobile user who participates in the mobile user's social interactions. The LS may have the capability to access the Internet or establish the local distributed mobile social network among neighboring users. The LS can also Opportunistic WLAN networks Cellular networks Wi-Fi access point Content Internet pool Base station Local server Centralized server Data flow disseminate the contents to nearby mobile users with a longer communication range greater than that of the mobile user. The device that the LS take is storage-rich and has a battery with plenty of power. Since the User-to-LS domain is featured by the local attribute, the LS provides multimedia services, local guidelines, and advertisements, and posts the local customer's reviews to make other customers better understand the properties of the store.

User-to-User Domain : When users are in a mobile environment where either continuous Internet services may not be guaranteed or users can directly exchange contents with each other in the vicinity, User-to-User communications plays an uppermost role. In a local area, users with similar social preferences may want to share their multimedia contents with each other. They can utilize Bluetooth to establish a temporary connection for content sharing without the assistance of the Internet, where the communication range is from 1–100 m in the local area, and multi hop communication is applied. The goal is to share contents among users or social friends, or cooperatively complete some specific activities.

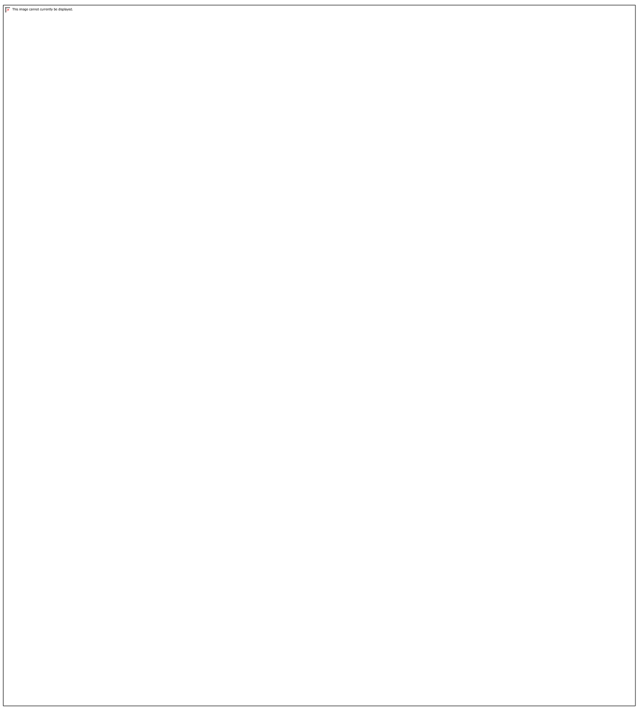

Fig1. Multimedia-oriented mobile social network.

3. SECURITY AND PRIVACY IN MMSN

Mobile social network systems, such as WhozThat and Social Aware, exchange users' social network identifiers between devices using short-range wireless technology like Bluetooth. In contrast, a mobile device in client-server mobile social network systems, like Brightkite and Loopt, notifies a centralized server about the current location of the device. By querying the server, mobile devices in these client-server systems can find nearby users, information about these nearby users, and other items of interest. The following will discuss security and privacy problems associated with mobile social network systems.

3.1 PRIVACY DISCLOSURE

Since users are not willing to disclose their own unique and private information including multimedia contents to others, particularly strangers, privacy preservation is more important in MMSN, where the contents may be highly related to users' privacy, like identities, locations, preferences, and social relationships. Generally, cryptography is implemented to protect the contents from being directly eavesdropped by outside attackers when transmitting and processing. On the other hand, an attribute-based access policy could be used to confine other users' access capabilities. X. Liang et al [4] exploit secure profile matching to prevent users' unique and private information from being directly exposed to others when users are matching their profiles. In spite of these cryptographic mechanisms, some private information attached to users' friends can still violate that user's privacy. When a user Bob queries some specific contents to the CS or his social friends, the query request might reflect Bob's preferences. Then the CS or other users might infer Bob's other attributes, violating his privacy. Sometimes, users are not even aware of the attachment of their privacy, and do not purposely protect themselves. As a result, to achieve privacy can guarantee users a secure MMSN and provide a better multimedia service experience.

3.2 TRUST RELATIONSHIP

Trust is a typical feature of social-based applications in an MMSN, since the contents shared among social friends are more trustworthy than those from strangers. In a mobile or local environment, to identify content authenticity and trustworthiness is still crucial since many delivered contents are from strangers instead of social friends. Particularly, in a local service evaluation, users may not fully trust reviews from strangers since a stranger's preferences could be quite different, and the reviews might not be useful. If the reviews can be related to the reviewer's preferences, the trustworthiness would be significantly improved. However, the link ability between the comments and the reviewer's preferences might disclose the reviewer's privacy. Privacy should also be preserved when exploring trust to improve the service experiences of users. The major challenge of trust in an MMSN is how to build trust relationships among mobile users and provide trustworthy contents to them.

3.3 MALICIOUS ATTACKS

There may be malicious attackers in an MMSN who might launch attacks to either degrade network performance or violate legitimate users' information. In content sharing, a malicious user forges contents and shares fake ones with other users. And also during cooperation, malicious users might not contribute as much as other users pay or even launch denial of service attacks. Particularly, in the service evaluation within the User-to-LS domain, LS arbitrarily posts positive reviews and deletes negative ones, or colludes with some mobile users to forge comments. As a result, users cannot extract useful and correct information or review comments on target stores. In summary, security mechanisms should be adopted to resist malicious attacks and guarantee a secure MMSN for users.

4. SECURITY SOLUTIONS FOR MMSN APPLICATIONS

4.1 INFORMATION EXTRACTION APPLICATION

Information extraction is broadly applied in social networks and is an essential component of an MMSN. Definitely, querying desirable contents reflects the user's critical mind and is an uppermost target in an MMSN. Information extraction exist in User-to-CS, User-to-LS, and User-to-User domains deals to the desirable content types. Because the CS not only has the largest potential of storage, computation and communication, but also maintains the connections with worldwide content resources, contents from users could easily be shared together on the CS side. With the connections to the CS, users typically directly submit their information extraction request containing their preference.

Based on the requests from users, CSs search the server and select the appropriate contents for users. With the recent arrival of cloud computing, cloud servers represent the most highly engaged segment of content storage and processing, where cloud servers store the most of the multimedia contents and process them, considerably saving the storage and computation consumption of the original servers. In the meantime, the security and privacy issues are not trifling, since the cloud server may not be fully believed and may act as a malicious entity in an MMSN. First, a cloud server may be compromised by outside attackers. If all the contents are stored as the plaintext in the cloud server, content privacy would be violated. Several research efforts have been focused on the content privacy where the raw contents are encrypted and stored in the semi trusted cloud servers. The key issue is how to competently store the massive number of contents and effectively process them as well. Second, during the content query, if a user queries some contents with some specific features, such as key words and some other properties, the cloud server cannot complete the query since the stored contents are in the cipher text. Under these circumstances, some research efforts have been made to address these issues in the User-to-CS domain. The hidden vector encryption (HVE)-based range query scheme with privacy preservation can blind the query content in cipher text so that the servers, including semi-trusted cloud servers, cannot directly learn the exact query of users but can compute the query result in the cipher text. There are three phases: range query predicate construction, encrypted content upload, and range query. The content owner u_o first chooses an index vector $\mathbf{x}$ = (x1, …, xl) to symbol the content m, and encrypts m with the encryption key k_o. Meanwhile, k_o is encrypted under vector $\mathbf{x}$ with the CS's public key. Then the cipher text of the content is sent to cloud server 1, while the cipher text of k_o is sent to cloud server 2, where cloud servers 1 and 2 are independent entities. Then the query requester sets up the query token $\mathbf{w}$ with the query translator component. The requester then sends the query token to cloud server 2, where the query token and stored content index are cryptographically matched. Here, a predicate function over a set of binary

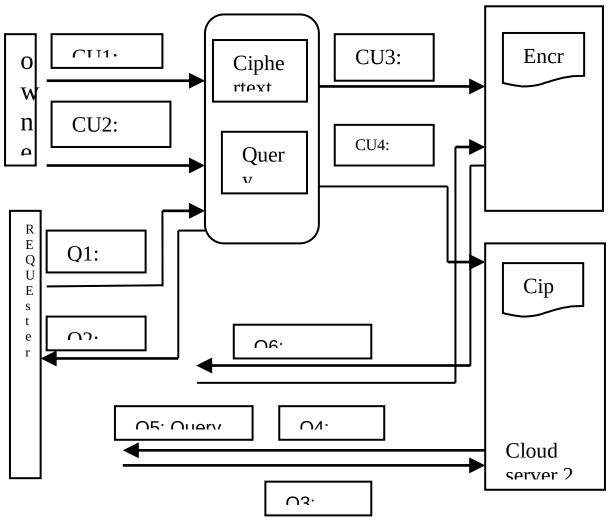

Fig. 3. ***Privacy-preserving range query in MMSN. CU denotes content uploading, and Q denotes query procedures.***

strings ∑ is F: ∑ {0, 1}, and F(X) = 1 if and only if X∈∑. A cryptographic function Query ($\mathbf{w}, \vec{\mathbf{x}}$) = k_o if and only if F($\vec{\mathbf{w}}$) = 1 (i.e., **w** ∈ **x**). As a result, at cloud server 2, if the query token matches some index, the corresponding encryption key k_o could be selected and firmly transmitted to the query requester. Finally, the query requester uses the index to get the cipher text of content m from cloud server 1 and decrypts it with k_o. While the token translator is automatically carried on and transparent to the CS, the query is not directly revealed. After the query requester gets the query token, the query content is hidden in the token. Therefore, the privacy of both content owner and query requester can be conserved.

4.2 SERVICE ESTIMATION

Service estimation is an attractive and value-added application in an MMSN. When users are in a shopping mall or on a commercial street, they might like to find features of local stores. One way is to search in web-based social networks, like Face book or eBay, via the Internet to browse other customers' reviews. These online reviews are not as real-time as possible since customers might not directly leave their reviews online. Since not all customers provide their reviews, the posted reviews might not properly reflect the service quality of the local stores. An emerging approach is to enable the LS to directly collect all customers' reviews and make them public to local customers, which is driven by the demands of both LSs and users if the LSs would also diffuse their advertisements to local users to attract them. The challenging issue is how to convince users and make them trust the posted reviews, since the trust relationship among local mobile users would not be very strong.

In the User-to-LS domain, there is no trusted authority to build up the trust relationships between users and LSs. How to provide trust evaluation for the LS is crucial, and would benefit both LSs and users. Furthermore, some malicious attackers might exist in the network and negatively impact the reviews. If the vendors become the attackers, they might forge some positive reviews, and delete or modify the negative ones. Furthermore, the attackers could submit fake review comments. In [4], Liang et al. propose a trustworthy service evaluation system to enable users to share their review comments in service-oriented mobile social networks (in the User-to-LS domain). Several tokens are generated by the LS and then circulated among users to synchronize their review submission behaviors. If a user would like to leave a review, he/she completes the review submission until he/she receives a token from either the LS or other users who have similar preferences. Then this user either directly submits a review and returns the token to the LS, or cooperates with other neighboring users who also want to submit reviews to the same LS in order to submit an integrated review. The signature and aggregate authentication techniques are adopted to maintain review integrity and efficiently verify the users' signatures. The LS maintains a token pseudonym list where each token is associated with a pseudonym that belongs to the user who most recently submitted a review with this token. When a new review is received, the list will be updated and periodically broadcast to all users in the communication range of the LS. After publishing a token, the LS cannot delete this token from the token pseudonym list even if a review is negative. The length of the review chain for every token determines the LS's modification capability; In addition, the privacy-preserving profile matching technique is utilized to help neighboring users find common preferences between them. These common preferences could facilitate them to establish a trust relationship. In this application, Sybil attacks, where an attacker abuses pseudonyms to produce multiple un linkable fake reviews in a short time, and review attacks, where attackers delete or modify reviews, can be resisted based on the specific token structure. To resist Sybil attacks, the time window is divided into time slots. If a user produces a massive number of reviews with the same pseudonym in a time slot, this user can easily be detected by the public. Therefore, Sybil attacks can be effectively detected, and the malicious reviews are rejected.

4.3 SPAM CONTENT SORTING

In a shopping mall or local area, many service providers disseminate their advertisements and flyers to customers, especially in the User-to-LS and User-to-User domains. In such a case, users may want to receive interesting service information instead of useless spam contents, particularly in a shopping mall or on commercial streets. For example, Bob is looking for the clearance jeans on a commercial street where he only requires the service contents about specific stores rather than restaurants or groceries. Intuitively, Bob could distribute some key-word-based filters containing his preferences to other users to block the unwanted contents and ensure the delivery of the useful ones. Thus, the selection of filter holders is of paramount importance in cooperative content filtering.. On the other hand, since the filters contain the key word contents that reflect the filter creator's preference, a user's privacy might be violated if directly distributing the filters to others. Therefore, protecting the user's key word contents from direct exposure to others is crucial. In [3], Zhang et al. propose a social-based spam filtering scheme for mobile social networks and consider the distribution and update.

Based on the investigation of social impacts, they devise a filter distribution mechanism where the filters are purposely sent to the filter creator u_i's social friends having several common attributes with $u_{i.}$ Since the social friends in a mobile environment would encounter u_i frequently, it is possible for the content senders to select them as the relay to disseminate the service contents to u_i. As a result, u_i's friends could block the spam contents in advance so that the network resources are extensively saved without useless or spam content delivery. Furthermore, the communication overheads of filter distribution are massively reduced since the filters are purposely distributed rather than random or epidemic distribution. To preserve a user's privacy, the distributed filters, including the key word of the creator's preferences, are encrypted in cipher text where bilinear pairing techniques are utilized. At the beginning, the filter creator u_i chooses a random number xi ∈Zq* as the private key SK_i and computes her public key $PK_i = 1/x_iP$. The filter of u_i's key word W_k is F_{ui},k =< W_{ui},k, λ_0 >,where

$$W_{u,,k} = \frac{H_1(Wk)}{X_i+H_1(W_k)} P, \lambda_0 = e(PK_i ,P)$$

Then F_{ui},k is distributed to u_i's social friends. Her social friends could be honest but curious users. When a content source u_s sends a packet with key word W_x to u_i and finds u_j as a potential relay, u_j could help u_i detect whether or not this packet is desirable. Here, W_x is encrypted as $\Lambda s = \lambda_1 + PK_i$, and

$$\lambda_1 = \frac{1}{H_1(W_x)} P$$

Then u_j checks e(Λs, W_{ui},k) ?= l0. If it holds, the keyword W_x passes the filter check, and the packet can be forwarded by u_j; otherwise, this packet will be blocked. Therefore, the private contents (i.e., the key word in the filter) are encrypted and protected from exposure to other users. To resist the filter forgery attack, a Merkle hash tree is utilized to authenticate the filters from the creator u_i. Specifically, u_i sets her key word list W_{ui} = W_{ui},1, …, W_{ui},K, where W_{ui}, k (1 ≤k≤ K) is the key word selected by ui, and located as a leaf node in filter tree FR_{ui}. During the authentication, the unique path information PH_k from the leaf node to the root node is used as the certificate for each independent key word (leaf node). Other users check whether or not the concatenated hash value of PH_k is equal to the root R_{ui}. With this scheme, the filter forgery attack is defended in the spam content filtering.

5. CONCLUSION

In this paper, we have introduced the MMSN architecture and recognized the security and privacy disputes. Furthermore, we have presented three MMSN applications, and concentrate on the security and privacy issues with sustaining effective countermeasures, counting privacy of content query, trust-based service estimate and privacy-preserving content filtering. At last, we have offered future research directions with reverence to privacy and secrecy in multimedia and multimedia-related mobile Sybil defense. We visualize that this research should support both service supplier and user in secure and privacy-conserves MMSNs.

REFERENCES

[1] K. Lin et al., "SocioNet: A Social-Based Multimedia Access System for Unstructured P2P Networks," IEEE Trans. Parallel Distrib. Sys., vol. 21, no. 7, 2010, pp. 1027–41.

[2] G. Cardone et al., "Socio-Technical Awareness to Support Recommendation and Efficient Delivery of IMSEnabled Mobile Services," IEEE Commun. Mag., vol. 50, no. 6, 2012, pp. 82–90.

[3] K. Zhang *et al.*, "SAFE: A Social Based Updatable Filtering Protocol with Privacy-Preserving in Mobile Social Networks," *Proc. IEEE ICC*, 2013, pp. 6045–49.

[4] X. Liang et al., "Security and Privacy in Mobile Social Network and Applications: Challenges and Solutions,"IEEE Wireless Commun., to appear.

[5] J. Troncoso-Pastoriza and F. Perez-Gonzalez, "Secure Signal Processing in the Cloud: Enabling Technologies for Privacy- Preserving Multimedia Cloud Processing," IEEE Sig. Process. Mag., vol. 30, no. 2, 2013, pp. 29–41.