Secure Caching of Application Data In Social Networks Based on User's Location

Sayali Parab[1], Purvi Prabhu[2], Snehal Sawant[3], Prof. Amruta Pokhare[4]
Department of Information Technology
[1,2,3,4] Atharva College of Engineering, Mumbai, India

Abstract- *Mobile edge computing has emerged as a promising solution that can provide computing and caching service to mobile users. This paper proposes the placement of edge nodes near mobile social users. Instead of needing to fetch content from the remote server, the content requested by mobile users can be directly provided by a nearby edge node. For this, a secure caching scheme to deliver mobile social data needs to be provided. This paper presents a secure edge caching scheme for mobile data in social networks based on the trust degree of edge nodes. Firstly, a trust evaluation mechanism is used to evaluate the reliability of each edge node. Then, each content generator selects the optimal edge node to cache the content and determines the optimal caching size, where the interactions between edge nodes and mobile users are modelled by a matching game approach.*

Keywords- Mobile social networks, mobile data, edge computing, security, trust evaluation, multiple concurrent contents.

I. INTRODUCTION

Frequently accessed data performance is generally improved by storing it in a small amount of faster, more expensive memory, generally called cache, which is rapidly accessible and separate from the bulk storage. When a webpage is visited, the requested files are stored in the user's computing storage in the browser's cache, clicking back and returning to a previous page enables your browser to retrieve most of the files it needs from the cache instead of having them all resent from the web server. This approach is called read cache. The browser can read data from the browser cache much faster than it can reread the files from the webpage. (1)

However, the deliveries of contents for mobile social data are hard to obtain the satisfied performances with the increasing scale of mobile social networks. Firstly, since the content servers are usually located at remote area, it delays the ability of mobile users to fetch contents. Secondly, the backbone is overloaded by the deliveries for a large number of contents, where the contents have been the main part of the current internet traffic. To overcome these two problems for mobile social data, the edge computing is a very promising way, where content caching is a practical application of edge computing. With the edge computing technology, the contents cached using edge computing is close to mobile users. Due to the short distances between the edge computing and mobile users, the delay to obtain contents can be significantly reduced. In addition, since contents can be acquired from adjacent edge computing instead of remote servers, the traffic on the backbone can be efficiently decreased (3-4).

In this paper, we present a secure caching scheme with edge computing to store multiple concurrent contents for mobile social data based on a one-to-many matching game. Firstly, to guarantee the contents that can be securely cached on edge nodes, a trust evaluation mechanism, based on the mobile user's geo location, is introduced to assess the reliability of each edge node, where the trust derivation consists of the evaluation of the direct trust. Secondly, each mobile user selects the optimal edge node and determines the proper caching size to store the contents. The interactions between edge nodes and mobile users are modelled by a matching game approach.

II. EASE OF USE

The system will consist of a Java program which will automatically run at the background while the user accesses some application. The user is not required to do anything to start the process of caching. It will be automatically done by the system when some application is used by the user.

III. SYSTEM DESIGN

To resolve the existing work we propose a new approach which will be helpful to keep the users data more secure and cost efficient. The proposed work will solve the problem of attacks on the user's data taking into consideration the size and the cost of the edge node using a matching algorithm.

A. Block Diagram

Figure 1 below shows the System Block Diagram which serves as the framework of the system.

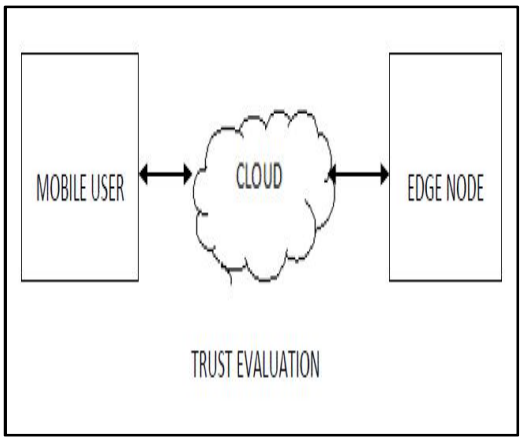

FIGURE 1: System Block Diagram

The Mobile User, Cloud and the Edge Node are the main components of the system, mobile user using his mobile device as the content generator and edge nodes i.e. the caching nodes located at the edge of cloud storage server.

Figure 2 below explains the detailed steps of implementation of the system.

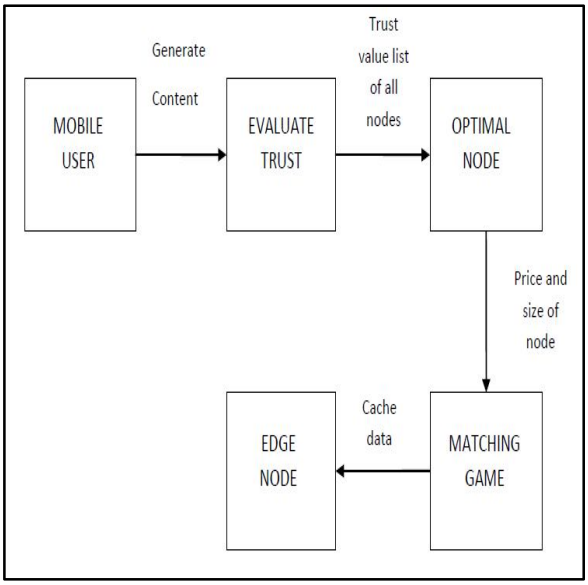

FIGURE 2: Detailed Block Diagram

The detailed steps of implementation of the system are as follows –

1. The mobile user acts as a content generator and uses the desired application to generate content.
2. It then implements the trust evaluation mechanism in order to choose the desired caching node to cache its data.
3. After choosing the optimal caching node, it uses a matching game algorithm to connect to the said node and cache the required data

B. Use-Case Diagram

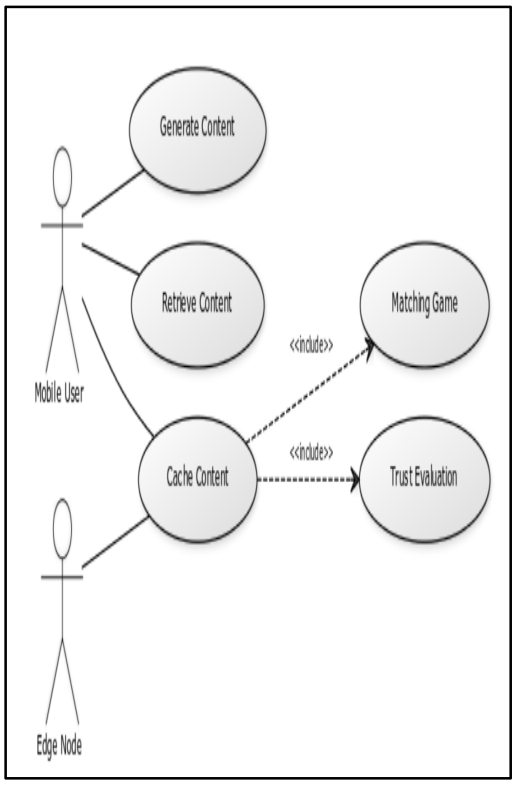

FIGURE 3: Use Case Diagram

Figure 3 shows the use case diagram of the proposed system which describes the role of the mobile user and the edge node.

1. Mobile User :

The mobile user accesses the application which he needs. As the application is used, the content is generated which is to be cached so that the same content is accessible to the user next time easily without any delay.

2. Edge Node :

The nodes at the edge of the cloud are selected to store the cache data so that the data is easily accessible to the user. To select the most secure node a trust evaluation mechanism is used which determines the trust a user has on each node and accordingly, depending on the trust, size and cost of the node the most optimal node for caching the generated content is selected and matching game algorithm is used to connect the node to the cloud.

C. Activity Diagram

Figure 4 describes the activity diagram of the system.

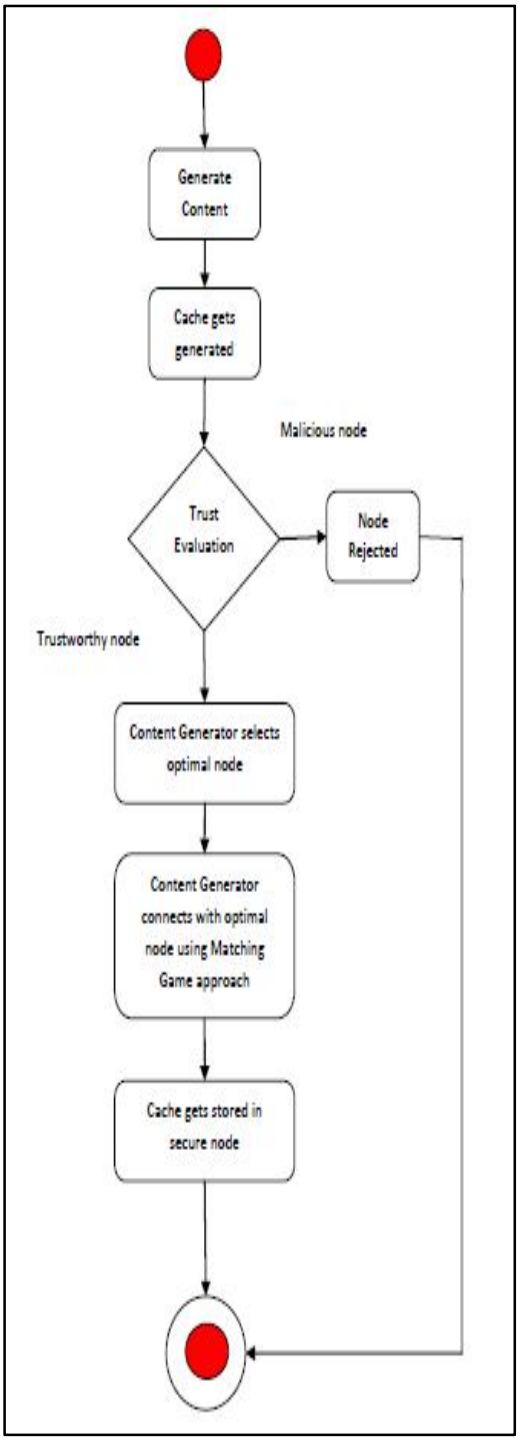

FIGURE 4: Activity Diagram

Firstly the content is generated which is then cached. Then the trust evaluation mechanism is used to determine the direct and indirect trust of each node. If the node is a malicious node then it is excluded and the node which has the highest trust and which is most optimal is selected by the content generator. This optimal node is connected to content generator using the matching game approach. The cache then gets stored in the secure node and is accessible whenever needed.

D. Sequence Diagram

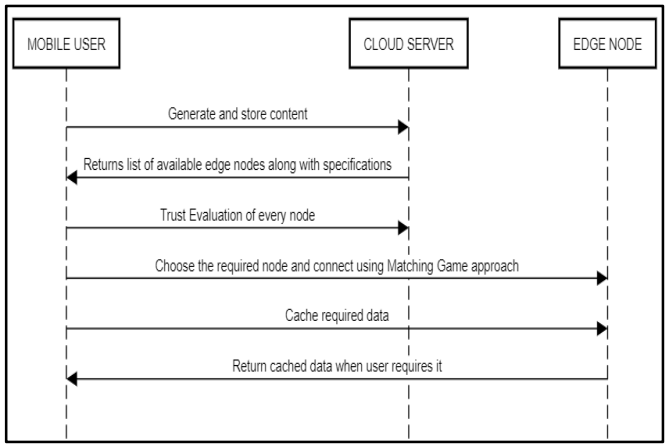

FIGURE 5: Sequence Diagram

FIGURE 5 given above gives a clear idea of how the objects such as mobile user, cloud server and edge node will work together in a sequence. When the mobile user will use an application, he will generate content. This content will be stored at the cloud server initially. The cloud server will then return the list of available nodes at its edge to the mobile user. The mobile user will then evaluate the trust of every edge node in the list by calculating their direct and indirect trust. After trust calculation, mobile user will select the required node according to his specifications and connect with it using the matching game algorithm. It will then cache the required data at the selected node. Now, when the user will use the application again and try to find this specific content, the edge node will return the appropriate cached content to the user device.

IV. EXPECTED RESULTS

This paper aims to provide secure and reliable caching services to mobile users of social networking sites through edge computing. Trust evaluation mechanism will be designed as such so as to select the optimal edge node for caching the required data. Lastly, matching game approach will be used to connect the content generator and the selected optimal edge node.

V. CONCLUSION

In this paper, a matching game based trust edge caching for mobile big data in social networks will be provided. A trust evaluation mechanism will be introduced first to show the reliability of each edge node, where the trust

degree of each edge node is analysed by the direct trust and indirect trust. The direct trust is based on the direct historical interaction while the indirect trust is according to the recommendations from other mobile users. Then mobile users can select the optimal edge nodes to store the contents and determine the optimal caching size to request, where the interactions between edge nodes and mobile users are modelled by the matching game. Finally, the proposed scheme can improve the quality of experience of mobile users and protect the network from the attacks of malicious edge nodes.

REFERENCES

[1] Margaret Rouse, Stacey Peterson and Brien Posey, "cache (computing)", https://searchstorage.techtarget.com/definition/cache, August 2018.

[2] Q. Xu, Z. Su, Q. Zheng, and B. Dong, "Secure content delivery with edge nodes to save caching resources for mobile users in green cities", IEEE Transactions on Indrustry Informatics, 2017, DOI: 10.1109/TII.2017.2787201.

[3] L. Hu, H. Wen, B. Wu, J. Tang, and F. Pan, "Adaptive base station cooperation for physical layer security in two-cell wireless networks," IEEE Access, vol. 4, pp. 5607-5623, 2016.

[4] Y. Chang, H. Liu, L. Chou, and Y. Chen, et al., "A general architecture of mobile social network services," in Proceeds of. International Conference on Convergence Information Technology, Gyeongju, Korea, pp. 151-156, Nov. 2007.

[5] Qichao Xu+, Zhou Su+, and Minghui Dai+ +School of Mechatronic Engineering and Automation, Shanghai University, Shanghai, China, "Trustworthy Caching for Mobile Big Data in Social Networks", in IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS): BigSecurity 18: The Fourth International Workshop on Security and Privacy in Big Data, 2018.

[6] Z. Su, Q. Xu, Q.Yang, and F. Hou, "Edge caching for layered video contents in mobile social networks", IEEE Transactions on Multimedia, vol. 19, no. 10, pp. 2210-2221, 2017.