TRUST-BASED VIDEO MANAGEMENT FRAMEWORK SYSTEM FOR SOCIAL MULTIMEDIA NETWORK

S.SHANMUGAPRIYA , NAGINA.N

Abstract— Social Multimedia Networks (SMNs) have attracted much attention from both academia and industry due to their impact on our daily lives. The requirements of SMN users are increasing along with time, which make the satisfaction of those requirements a very challenging process. One important challenge facing SMNs consists of their internal users that can upload and manipulate insecure, untrusted and unauthorized contents. For this purpose, controlling and verifying content delivered to end-users is becoming a highly challenging process. So far, many researchers have investigated the possibilities of implementing a trustworthy SMN. In this vein, the aim of this paper is to propose a framework that allows collaboration between humans and machines to ensure secure delivery of trusted videos content over SMNs while ensuring an optimal deployment cost in the form of CPU, RAM, and storage. The key concepts beneath the proposed framework consist in i) assigning to each user a level of trust based on his/her history, ii) creating an intelligent agent that decides which content can be automatically published on the network and which content should be reviewed or rejected, and iii) checking the videos' integrity and delivery during the streaming process. Accordingly, we ensure that the trust level of the SMNs increases. Simultaneously, efficient Capital Expenditure (CAPEX) and Operational Expenditures (OPEX) can be achieved.

I. INTRODUCTION

The recent advances in the Internet have resulted in the emergence of many web applications and social multimedia networks (SMN). These applications (e.g., Facebook, Twitter, and Google) have revolutionized the use of the Internet as a tool to interconnect people over the world. The features implemented by these service providers have been making communication between people easier. Service providers have granted to the users more flexibility for interacting among themselves and exchanging different social information. Thanks to these services, users can easily discuss their ideas and opinions remotely, publish new articles, and meet new persons. Moreover, they have allowed business and organizations to advertise for their products over the world and to directly contact their customers. In addition to these social networks, other web applications, such as Youtube, Dailymotion, and Vimeo, have enabled the exchange of different contents, including text, images, and videos among different entities connected to their services. The evolution of the Internet and distributed systems has led researchers to implement applications that serve video on demand (VOD) on top of the peer-to-peer (P2P) networks

VOD and videos live streaming systems are gaining momentum in SMN. They have enabled the appearance of many multimedia-centric services such as video conferencing applications, online meeting applications, massive open online courses (MOOC) as well as other use cases in e-health and e-teaching [4]. Such services attract and connect millions of users worldwide. The providers of these services have enabled countless features that allow users to interact among themselves by creating and sharing different contents (e.g, videos, text, and images). However, by allowing this, the nodes composing the social networks, users and machines, generate a huge amount of data, which can be uncontrolled, unsecured and untrusted [5], [6]. Such amount of generated data are causing a congestion to the networks [7], [8] and posing a new security challenge to the service providers: I becomes hard to handle and analyze all content traversing their

S. Shanmugapriya , Associate Professor, Department of Computer Applications,Erode Sengunthar Engineering College (Autonomous), Perundurai, Erode. (Email : riyashanmu@gmail.com)
N.Nagina , PG Scholar , Department of Computer Applications, Erode Sengunthar Engineering College (Autonomous), Perundurai, Erode. (Email : naginan808@gmail.com)

networks. To tackle this problem, many research efforts have been conducted so far for mitigating the upload of malicious data to SMNs. Diverse data analytics applications have been proposed and developed with the goal to create a trustworthy SMN [9], [10].

The researchers' vision of trustworthy SMNs [11] lies in achieving certainty, authenticity, and security of data exchanged throughout social network nodes [12], [13]. In this vein, many trust models and reputation systems have emerged [14]–[16] with the goal to limit the spread of unsecured data. Generally, trust models and reputation systems are designed to assign a score to each entity in the network and establish trust among them. This score may help users to make a proper decision on buying an item from an online store, selecting a service provider or recommending a service to other users. Additionally, the trust score provides decisional systems with the needed information to execute adequate actions, such as the implementation of certain policies that restraint an entity from using some resources or accessing some services. The main features that should be taken into consideration while defining a trust model are as follows:

_ User history: The only way to predict user behavior is to study and analyze all generated content by different users during their interactions in the network [17]. The user history records may contain relations and links between data [18], these links are valuable for the data analytics applications in order to offer a good user experience.

_ Trust calculation: A user's level of trust is one of the important metrics that should be taken into consideration when analyzing users' data. The computation of this value includes the selection of various parameters that characterize the manipulated data [19]. For this reason, there is a need to suggest a realistic model that can capture the characteristics of uploaded data based on the historical behavior of users.

_ Users collaboration: Based on the observation that human intelligence is one of the main keys to effectively detect and remove untrusted data, many algorithms and applications have been recently devised for detecting and measuring users' collaborations rate [20]. These algorithms and applications allow users to rate different social multimedia items. Then, the system is able to collect these feedbacks, applies some filtering methods and executes different needed actions.

_ Secure content delivery: In a trustworthy social network, every bit of data should be under control. In other words, starting from any node in the network (e.g, user, mobile, or server), the path that the data take to arrive at another node should be secured [21], [22].

II. LITERTURE SURVEY:

A popularity-driven video discovery scheme for the centralized P2P-VoD system the popularity of network, P2P-based Video on Demand (VoD) has become one of the main services in Internet. However, due to the huge amount of videos, how to access the video quickly is important since it affects the subscriber's experience. In this paper, a popularity-driven storing model is proposed to fasten the video discovery for a centralized P2P-VoD system. All videos are stored in a binary tree in the server according to their popularities. Experimental results show that this scheme works well in terms of discovery delay and resource utilization

A Comprehensive Methodology For Managing Social Network Videos In Trusted Environments

III. EXISTING SYSTEM:

Machine learning (ML) based approach is used in [19] to calculate the trust score for the different nodes of the social network. The logistic regression is used to train the neural network. The main reason beneath using such a model is the flexibility of ML solutions that can be adapted to different networks and platforms. The authors also introduced a method to effectively select the features that describe the data. In the same way, the authors in [27] used ML-based algorithms to mine the trust and distrust relationships in a social web application. In order to train their model to do some predictions, they introduced four inputs factors. The first factor, named Knowledge-based trust, combines the number of satisfactions between two given nodes. The second factor, named similarity-based trust, shows the degree of similarity between truster and trustee. The third factor, named reputationbased trust, represents the social importance of an entity in the network. Finally, the fourth factor, dubbed personality-based trust factor, shows a user's tendency to trust another user.

Authors in [24] proposed a method based on user cosine similarity [28] in order to calculate the trust value. This calculated value can be used to filter the neighbors and predict a recommendation items to another similar user. In their model, the authors considered that the trust value is transitive and can be transferred from a user to another. Wang et. al., in [25] proposed a trust model based on a Bayesian trust algorithm for self-organizing networks. The main idea behind this method is counting the number of successful and unsuccessful messages. In this work, the authors presented the trust as a tree dimensions vector. The first dimension of the vector is the connectivity, which is the capability of a node to connect another node in the network. The second dimension is fitness. It describes the behavior of a node and can help in detecting malicious nodes. The last dimension is the satisfaction, this parameter shows how much a node is satisfied by the intermediate nodes. By computing the parameters of this vector, each node can calculate the vector trust of other nodes and decide to accept or reject a recommendation from them.

Last but not least, authors in [26] exploited the graph theory to compute the trust and distrust in a network. Their work was inspired by the computation of path probability in random graphs [29]. The graph's edges represent the probability that a path exists between user A and user B. On the other hand, the distrust was inspired by spring embedding graph layout algorithms. The combination of these two algorithms allows the proposed trust model to pull trusted nodes and regroup them in a form of trusted cluster, conversely, un trusted nodes are pushed away.

Disadvantages:

- In the existing work, the system does not Driving Mechanism of User's Personal Characteristics.
- This system is less performance due to lack of video uploading decision process (VUDP) module.

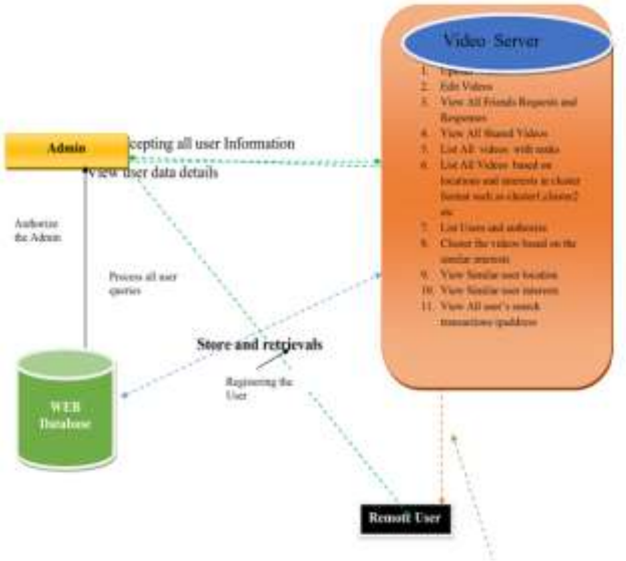
IV. POPOSED SYSTEM:

- User history: The only way to predict user behavior is to study and analyze all generated content by different users during their interactions in the network [17]. The user history records may contain relations and links between data [18], these links are valuable for the data analytics applications in order to offer a good user experience.
- Trust calculation: A user's level of trust is one of the important metrics that should be taken into consideration when analyzing users' data. The computation of this value includes the selection of various parameters that characterize the manipulated data [19]. For this reason, there is a need to suggest a realistic model that can capture the characteristics of uploaded data based on the historical behavior of users.
- Users collaboration: Based on the observation that human intelligence is one of the main keys to effectively detect and remove untrusted data, many algorithms and applications have been recently devised for detecting and measuring users' collaborations rate [20]. These algorithms and applications allow users to rate different social multimedia items. Then, the system is able to collect these feedbacks, applies some filtering methods and executes different needed actions.
- Secure content delivery: In a trustworthy social network, every bit of data should be under control. In other words, starting from any node in the network (e.g, user, mobile, or server), the path that the data take to arrive at another node should be secured [21], [22].

Advantages:

- Component allows the trans coding of the uploaded videos to different resolutions using software's such as FFMPEG.
- To The system is more effective due to presence of SOCIAL MULTIMEDIA
- NETWORK GENERIC FRAMEWORK.

V. ARCHITECTURE DIAGRAM


Video Server
1. Upload
2. Edit Videos
3. View All Friends Requests and Responses
4. View All Shared Videos
5. List All videos with ranks
6. List All Videos based on locations and interests in cluster format such as cluster1,cluster2 etc
7. List Users and authorize
8. Cluster the videos based on the similar interests
9. View Similar user location
10. View Similar user interests
11. View All user's search transactions ipaddress
Admin
cepting all user Information
View user data details
Authorize the Admin
Process all user queries
Store and retrievals
Registering the User
WEB Database
Remott User

VI. IMPLEMENTATION

In this module, the Admin has to login by using valid user name and password. After login successful he can do some operations such as upload videos, view uploaded videos, view the searching history, view all image ranking and view all users, search videos and logout.

1) Upload Videos:

In this module, the admin can upload n number of videos. Admin want to upload new image then he has enter some fields like image name, image color, image description, image type, image usage, browse the image file and upload. After uploading successfully he will get a response from the server. Initially new uploaded image rank is zero. After viewing that image rank will re-rank.

2) Search History

This is controlled by admin; the admin can view the search history details. If he clicks on search history button, it will show the list of searched user details with their tags such as user name, user searched for Video name, time and date.

3) Vote of videos

In user's module, the admin can view the list of vote videos. If admin click on list of ranking videos, then the server will give response with their tags videos and interests or reviews and rank of videos.

4) User

In this module, there are n numbers of users are present. User should register before doing some operations. And register user details are stored in user module. After registration successful he has to login by using authorized user name and password. Login successful he will do some operations like View your Details,Search Friend and Friend Request,View All Friends, Search for videos based on the video contents and give your interest for the videos and Share, View my search History ,View Similar users in the same trusted locations, View user interests on the video,View Top K interested videos(If Top K is 5,then list all first five ranked videos),Search Friend and Friend Request ,View All Friends.

VII. SCREENSHOT

VIII. FUTURE ENHANCEMENT

In future the efficiency of the proposed algorithm in terms of publishing the good contents and forbidding the bad ones. Also, the simulation results demonstrate the efficiency of proposed algorithms in terms of minimizing the incurred computational cost.

IX. CONCLUSION

Social multimedia networks are gaining a lot of momentum and their services are becoming the most popular ones among the community of Internet users. The data generated and exchanged by users of these networks become diverse. They include videos, documents, text, and pictures. Unfortunately, there are users that can insert insecure, untrusted and unauthorized contents. Thus, there is need for an effective way to control and verify the exchanged content. In this work, we focused on how to ensure that the users upload only secured, trusted and authorized videos to the social multimedia networks. We therefore proposed a complete framework that takes into account different aspects to attribute trust values to both users and content and to accordingly secure video streaming. The proposed framework has been designed in a way to reduce the resources utilization in terms of CPU, RAM, and storage.

Moreover, we proposed a video uploading decision process module that leverages the historical behaviors of users for making the right decisions on either allowing or denying the upload of videos. This module uses an infinite discrete Markov decision process (DMDP) for taking those decisions. Also, this module can decide for either to analytically check the contents or send them to external reviewers before publishing them or forbidding their publication. The simulation results demonstrate the efficiency of the proposed algorithm in terms of publishing the good contents and forbidding the bad ones. Also, the simulation results demonstrate the efficiency of proposed algorithms in terms of minimizing the incurred computational cost.

X. REFERENCES

[1] L. Gao, H. Ling, X. Fan, J. Chen, Q. Yin, and L. Wang, “A popularitydriven video discovery scheme for the centralized p2p-vod system,” in 2016 8th International Conference on Wireless Communications Signal Processing (WCSP), Oct 2016, pp. 1–4.

[2] W. Chang and J. Wu, “Social vod: A social feature-based p2p system,” in 2015 44th International Conference on Parallel Processing, Sept 2015, pp. 570–579.

[3] T. Taleb, N. Kato, and Y. Nemoto, “Neighbors-buffering-based videoon- demand architecture,” Signal Processing: Image Communication, vol. 18, no. 7, pp. 515 – 526, 2003. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0923596503000390

[4] T. Taleb and N. Taleb, “System and method for creating multimedia content channel customized for social network.” Patent PCT/US2011/049 159, Nov, 2011.

[5] Statista. Social media usage worldwide. [Online]. Available:https://www.statista.com/study/12393/social-networks-statista-dossier/

[6] G. Noh, H. Oh, K. h. Lee, and C. k. Kim, “Toward trustworthy social network services: A robust design of recommender systems,” Journal of Communications and Networks, vol. 17, no. 2, pp. 145–156, April 2015.

[7] T. Taleb, A. Ksentini, M. Chen, and R. Jantti, “Coping with emerging mobile social media applications through dynamic service function chaining,” IEEE Transactions on Wireless Communications, vol. 15, no. 4, pp. 2859–2871, April 2016.

[8] T. Taleb and A. Ksentini, “Impact of emerging social media applications on mobile networks,” in 2013 IEEE International Conference on Communications (ICC), June 2013, pp. 5934–5938.

[9] L. Yang, Z. Zhang, W. Tian, and Q. Chen, “Advance on trust model and evaluation method in social networks,” in 2012 Sixth International Conference on Genetic and Evolutionary Computing, Aug 2012, pp.9–14.

[10] X. Liang, X. Lin, and X. S. Shen, “Enabling trustworthy service evaluation in service-oriented mobile social networks,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp. 310–320, Feb 2014.

[11] M. K. Rahman and M. A. Adnan, “Dynamic weight on static trust for trustworthy social media networks,” in 2016 14th Annual Conference on Privacy, Security and Trust (PST), Dec 2016, pp. 62–69.

[12] S. Hussain, N. Honeth, R. Gustavsson, C. Sandels, and A. Saleem, “Trustworthy injection/curtailment of der in distribution network maintaining quality of service,” in 2011 16th International Conference on Intelligent System Applications to Power Systems, Sept 2011, pp. 1–6.

[13] A. Ganz and A. Kumar, “A systems approach to teaching trustworthy computing,” in 2007 37th Annual Frontiers In Education Conference - Global Engineering: Knowledge Without Borders, Opportunities Without Passports, Oct 2007, pp. S1C–15–S1C–18.

[14] S. Hall, W. McQuay, and K. Littlejohn, “A trustworthiness evaluation framework for distributed networks,” in 2012 IEEE National Aerospace and Electronics Conference (NAECON), July 2012, pp. 51–56.

[15] S. Hall and W. McQuay, “Fundamental features of a unified trust model for distributed systems,” in Proceedings of the 2011 IEEE National Aerospace and Electronics Conference (NAECON), July 2011, pp. 139–145.

[16] C. Jia, L. Xie, X. Gan, W. Liu, and Z. Han, “A trust and reputation model considering overall peer consulting distribution,” IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, vol. 42, no. 1, pp. 164–177, Jan 2012.

[17] K. Das and S. K. Sinha, “Essential pre-processing tasks involved in data preparation for social network user behaviour analysis,” in 2017 International Conference on Intelligent Sustainable Systems (ICISS), Dec 2017, pp. 28–32.

[18] R. Wang and G. Chen, “Mining negative links between data clusters,” in 2015 IEEE International Conference on Communication Problem- Solving (ICCP), Oct 2015, pp. 520–523.

[19] W. Yuji, “The trust value calculating for social network based on machine learning,” in 2017 9th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC), vol. 2, Aug 2017, pp. 133–136.

[20] G. Zhao, X. Qian, and X. Xie, “User-service rating prediction by exploring social users’ rating behaviors,” IEEE Transactions on Multimedia, vol. 18, no. 3, pp. 496–506, March 2016.

[21] Y. Tian, J. Srivastava, T. Huang, and N. Contractor, “Social multimedia computing,” Computer, vol. 43, no. 8, pp. 27–36, Aug 2010.

[22] J. Sang and C. Xu, “On analyzing the ’variety’ of big social multimedia,” in 2015 IEEE International Conference on Multimedia Big Data, April 2015, pp. 5–8.

[23] F. Jabeen, Z. Hamid, A. Akhunzada, W. Abdul, and S. Ghouzali, “Trust and reputation management in healthcare systems: Taxonomy, requirements and open issues,” IEEE Access, vol. 6, pp. 17 246–17 263, 2018.

[24] T. Phukseng and S. Sodsee, “Calculating trust by considering user similarity and social trust for recommendation systems,” in 2017 12th International Conference on Intelligent Systems and Knowledge Engineering (ISKE), Nov 2017, pp. 1–6.

[25] E. K. Wang, Y. Li, Y. Ye, S. M. Yiu, and L. C. K. Hui, “A dynamic trust framework for opportunistic mobile social networks,” IEEE Transactions on Network and Service Management, vol. 15, no. 1, pp. 319–329, March 2018