An Efficient Automatic Content Filtering and Verification Video Publish on Social Multimedia Networks

Dwarapudi E Manikanta Prabhuvu[1], Dr. U. Nanaji[2]
[1]*PG Scholar, Dept. of computer science and engineering, Avanti institute of engineering and Technology narasipatnam Vishakhapatnam Andhra Pradesh*
[2]*Professor, CSE-HOD, Dept. of computer science and engineering, Avanti institute of engineering and Technology narasipatnam Vishakhapatnam Andhra Pradesh*

Abstract **- Because of their effect on our everyday lives, social multimedia networks (SMNs) have drawn a lot of interest from academia and industry. The demands of SMN users are rising; making meeting those demands a difficult job. Internal users who can upload and exploit vulnerable, entrusted, and unauthorized content are one of the most significant challenges that SMNs face. Controlling and verifying content delivered to end-users is becoming an increasingly difficult activity the aim of this project is to propose a system for human-machine collaboration to ensure safe delivery of trustworthy video content over SMNs while minimizing deployment costs. The proposed framework's main concepts include: I assigning a degree of trust to each user based for accessing the videos basing on his previous history using the concept of artificial intelligent agent which takes care of publishing on the network and verifying the videos' integrity and delivery during the streaming process it leads to trouble our this approach there will be a center line authority that check and monitor the activity of the user and basing on it ethnicity the user gives the access permission to the videos maintaining the trust of activity performance by end user.**

Index Terms **- Big Data, Proxy Re encryption, Storage Path, Cloud Storage, Sensitive Data.**

I.INTRODUCTION

The recent advances in information sharing have resulted in development of many web applications and communication between people easier. Users now have more social multimedia networks thanks to service providers (SMN). These apps (such as Facebook, Twitter, and Google) have revolutionised the way people use the Internet to communicate around the world. These service providers' features have given them the ability share and exchange various social data. 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. These social networks, other web applications like YouTube, Daily motion, and Vimeo, have enabled the exchange of different contents, including text, images, and videos among different entities connected to their services. Researchers have implemented applications that serve video on demand (VOD) on top of peer-to-peer (P2P) networks as the Internet and distributed systems have evolved [1]–[3]. In SMN, VOD and video live streaming services are gaining traction. Many multimedia-centric services, such as video conferencing applications, online meeting applications, and huge open online courses, made things possible by them (MOOC) as well as other use cases in e-health and e-teaching [4]. 1Such services draw and link millions of people all over the world. These services' providers have enabled a slew features which can connect between people and sharing the content (e.g, videos, text, and images). 7 However, in this process it generates massive amount of data being generated by the nodes that make up social networks, users, and computers and these are unregulated, unsecured, and untrustworthy [5], [6]. Such a large size produced data is called clogging networks [7], [8], and presenting a new security problem for service providers: it becomes difficult to manage and evaluate all traffic passing through their networks. 1 Many research efforts have been made so far to mitigate the upload of malicious data to SMNs in order to address this issue. Various data analytics technologies have been proposed and developed with the aim of

developing a reliable SMN [9], [10]. In this paper there was and implementation of vision trustworthy [11] is to achieve data security through social nodes [12], [13]. 9 there are many trust models which are been implemented [14–16] have emerged very important, with the intention to reduce the data. Generally, reputed trust models 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, a ranking system is provided for making adequate task by which a necessary action can be taken by which we can implement some polices for accessing the resources

TRUST MODEL BIG DATA STROAGE

Some of the main features while defining the Trust model are mentioned below:

- 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 social media [17]. The user history records may contain relations and links between data [18], these links will be useful for data analysis in order to offer a good user experience.
- Trust calculation: A user Trust is very important metrics that should be used for data analysis and computation these values include various parameters for analysis of manipulated data [19] we need to consider a realistic model that can capture the characteristics of uploaded data based on the historical behavior of users.
- Users collaboration: Based on the observation the intelligence system tool is one of the key factors which can detect and remove entrusted data, many algorithms are been developed in past for evaluating the users' activity with collaborations rate [20]. Here the users can apply different selection process for buying multimedia items by our proposed algorithm

Secure content delivery: in social network each and every information is very important which need to be authenticated and monitored in trustworthiness from the users mobile or server or any device the communication should be secured [21], [22]. Making sure the data is send has be made sure that it is trusted video Currently, the well- known social media networks rely on their users to report unauthorized contents in order to take the different counter-measures. Till today there is no tool which can avoid sharing the trusted video. In this paper, we paper we implement a trust frame work for trusted videos access. The main goal of the generic framework is to create a system that is able to provide secure delivery of trusted videos content over social networks with low resources consumption in terms of CPU, RAM, and storage. Indeed, the proposed system reduces the resource utilization, and accordingly the cost, by analyzing only the video content that really needs to be analyzed. The proposed framework explores both the user history and users' collaboration for taking the decision to either make the analytical analysis or not. The framework contains a module that is responsible for calculating the level of trust of each user in the network. 1 Apart from the user trust calculation module, the generic framework includes: I a voting service that allows users to reward trusted clients while penalizing malicious users; a) an incentive module that rewards users for their cooperation; b) a secure videos module that ensures secure video delivery; and c) a video integrity checker service that ensures the integrity and timestamping of uploaded videos. In addition, a client-side adaptation of the video player is suggested 6 to accept the current framework's suggested features 1 The upgrade involves adding a new feature to the video player that allows it to interact with the video integrity checker and ensure that the chunks buffered during the streaming process have not been tampered with. Furthermore, the proposed generic framework has a video uploading decision process module that enables checking the quality of the uploaded videos before either accepting the publication or not. Besides the use of historical behavior of users, this module explores two techniques for checking the quality of the uploaded contents:

i) analytical checking of the uploaded videos; *ii*) review checking of the uploaded contents by a set of trusted users. Based these types of techniques cost the hard amount and these types of applications explore the users behivours, the main goal to take the decisions without involving those two techniques. Also, here we use *Decision Markova* model for taking the decisions to either publish or not an uploaded video. Thanks to DMDP, the module is able to decide to either analytically check the contents or send them

to an external reviewer before publishing or deny the publication of the uploaded contents.

II.RELEATED WORK

we briefly present the research works that are most relevant to our proposed framework including trust-worthiness and social interactions of SMNs. The majority of published research on social media trust has computed the trust degree among the nodes [19], [23]–[26]. In this approach the author has implemented the a frame work for n system trusts and user and the cost factor was analyzed for evaluating the trust influence. 1 The trust and reputation system (TRS) in e-Health was addressed by authors in [23]. They implemented a bidirectional approach between entities and subject to expectations. Moreover, the authors presented some possible trust attacks model, in particular, *i*) the bad mouthing attack that occurs when an entrusted entity tries to hurt the reputation of another entity; and *ii*) the collusion attack that emerges when a group of entities tries to boost each other's reputation.

A 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. Similarly, the authors of [27] mined the confidence and mistrust relationships in a social network application using ML-based algorithms. They added four input factors to their model in order to train it to make predictions. The number of satisfactions between two nodes is combined in the first factor, Knowledge-based confidence. The second element, similarity-based confidence, tests how similar the trusted and trustee are. 2 The third approach is reputation-based trust, reflects an entity's social values Finally, the fourth factor, known as the personality-based confidence factor, demonstrates a user's willingness to trust another user. In [24], the authors proposed a method for calculating the trust value based on user cosine similarity [28]. This estimated value 6can be used to filter the neighbors and predict which objects should be recommended to another consumer who is similar. 4 The authors assumed that the trust attribute is transitive and can be passed from one user to another in their model. In [25], Wang et al. proposed a trust model for self-organizing networks based on a Bayesian trust algorithm. The key concept behind this approach is to keep track of how many good and ineffective messages have been sent. In this work, the authors presented the trust as a tree dimensions' vector. The first dimension of the vector is the connectivity, which is basically used for 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. Finally, authors in [26] used graph theory to calculate network trust and mistrust. The calculation of path likelihood in random graphs [29] was the source of inspiration for their work. The probability of a path between user A and user B is represented by the graph's edges. Spring embedding graph layout algorithms, on the other hand, were the source of suspicion. 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, untrusted nodes are pushed away.

III.PROPOSED WORK

In this approach we have was proposed and created with the aim of creating a reliable SMN. The proposed version is vision of reliable SMNs is to achieve data exchange and security, and protection through social network nodes. 9 Many trust models and reputation structures have emerged in this vein, all with the intention of limiting the spread of unsecured data. In general, confidence models and reputation structures are two types of systems. Here we assign a score for each object in the network to build a trust between the nodes by this approach it will be helpful for end user to buy a product form selecting a service provider or recommending a service to other users. 1In addition, the confidence score provides decision-making processes by this they can take appropriate steps, such as enacting policies that prevent an individual from using certain resources or accessing certain services. The following are the key characteristics that should

be considered when designing a trust model: History of the
user: Only by studying and analyzing all created content by different users during their interactions can user behavior be predicted. 6in the internet The user history records may contain data relations and connections; these links are essential for data analytics applications to provide a positive 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. 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: Many algorithms and applications have recently been developed for detecting and measuring user partnerships, based on the observation that human intelligence is one of the main keys to effectively detect and eliminate entrusted data. in our proposed algorithm by using any type of device like (e.g, user, mobile, or server), the communication should be secured.

ADVANTAGES

- The system has efficient and verifiable method to update the cipher text if it is integrated by malicious users.
- The data security is more in the cloud server due to data integrity by data owner also.

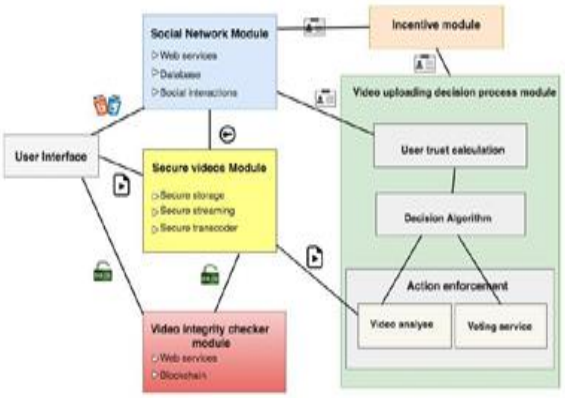

Fig 1: Proposed Architecture

IV.METHODOLOGY

Social network module (SNM)

This module is the first component that interacts with the users. It permits them to do all kind of social interactions, such as the upload of videos, the post of comments, and the sharing of different videos. This module is composed of many micro- services there are many types of modes of offer a user-friendly application that fulfills the end-users needs. The main micro-services are i) the web server that responds to the users' requests, ii) a database that stores all information of users and their generated content, iii) a caching micro- service for reducing the response time and allowing the users to have good experiences while interacting with the system, iv) a message broker that allows the communication between the different components, and v) a central authentication service that authenticates the users and gives them the right to request other services.

module (SVM)

This module allows authorized users to upload their media files to the secure storage, as well as it allows the social network users to watch the videos streamed on demand from the secure streaming. The SVM consists of three components: Secure storage: this component mainly works as follows: first of all, an authorized user sends an upload request to the SNM. Then, the social network module (SNM), more precisely the central authentication micro-service, generates and stores a unique token in the database, and then sends it to the user as a response. The user starts sending the video chunks to the storage server while including that token within the messages sent. The storage server (SS) checks the received token and then decides either to accept or reject the upload.
This component adopts the HTTP live stream (HLS) for serving diverse users with different resolutions adapted to their network bandwidth and devices. Also, this compo- nent uses the Rivest Cipher 4 (RC4) algorithm in order to encrypt the video chunks sent to the end users.
Secure transcoder: this component allows the transcoding of the uploaded videos to different resolutions using soft- wares such as FFMPEG. Each resolution is subdivided into small chunks of fixed time duration [35]. After the transcoding operation ends, the secure transcoder creates a hash for each chunk and sends that hash to the video integrity checker module (VICM). The VICM saves that hash in a public or private BLOCKCHAIN service as a

transaction. The hashed values will be used by the user video player to verify that the chunks received were approved by the system and the chunks were not modified from the time that a user uploaded the video to the secure storage.

Video integrity checker module (VICM)
The main feature of this module is to allow the times-tamping of the chunks generated from an uploaded video. This helps in checking the integrity of these chunks in the future. Formally, the VICM module saves the video content, its signature and its date-time of creation in a trusted and a shared database. Also, this module checks that the file has not been altered or modified thanks to Block chain technologies. Moreover, the service will be also used from a client (e.g, browser, tablet, smartphone, etc) to verify that the video chunks received were not altered during the streaming process.

Trust calculation module
This sub-module has the responsibility to compute the trustworthiness of different users. For this reason, it keeps monitoring the behavior of each user by taking into con- sideration his/her social interactions with other users. These social interactions include, but not limited to, the following parameters: i) the number of followers (NOF); ii) the number of true votes (NOTV) received from trusted users through the voting service sub-module; iii) the percentage of true reports (PTR) received from different users of the social network; iv) the percentage of likes (POL) received from the user network mainly his friends; and v) the average trust of published videos (ATPV).
For the sake of simplicity, the trust value of each user is computed using a weighted sum function of the different parameters. However, any more sophisticated method can be also used with slight modification. For instance, the entropy of Shannon can be also applied to these parameters for computing the trust degree of each user. In what follows, we will show how the trust values of users and videos are computed.

Data Owner
In this module, the data owner uploads their data in the social networking cloud server and performs the following operations Add Event Video, Add View All Videos

Social networking Servers
The Data Owner sends a request to Cloud Scheduler to provide services by assigning the task for any one cloud like View all users, Data owners and authorize, Add Event Category, view all videos with comments and score, Show video event score in Chart,

End User
In this module, the user has to get Registered to social networking Cloud server to access the Cloud services and need to Authenticate the user by Logging in by providing the User Name and operations the following operations such as View your Details and Search events by keyword based on event desc and display all events grouped by videos and make comments, Search events by category name and display all events grouped by videos and make comments., Search events by event tile and display all events grouped by videos and make comments.

- Security. The proposed scheme should be able to defend against various attacks such as the collusion attack. Where our approach will maintain the policy for data communication
- Verification. When a decryption process is stored in the form of cipher text, it trusts should be verified by other user and it should be validated for proper recovery

V. AUTHORIZATION

User Will Be Given Authorization by The Authority to Reduce the Risk of Leakage

VI. RESULTS AND DISCUSSION

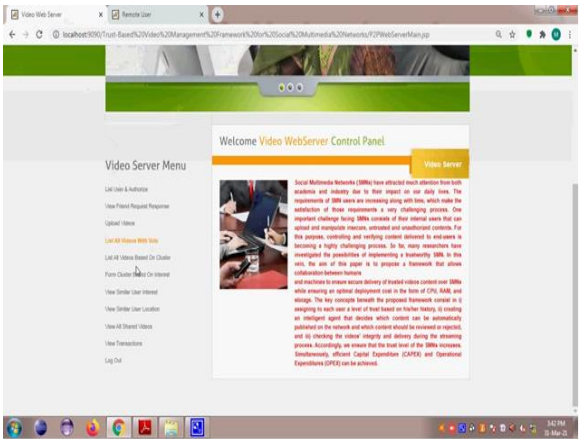

Fig2: - home page video server

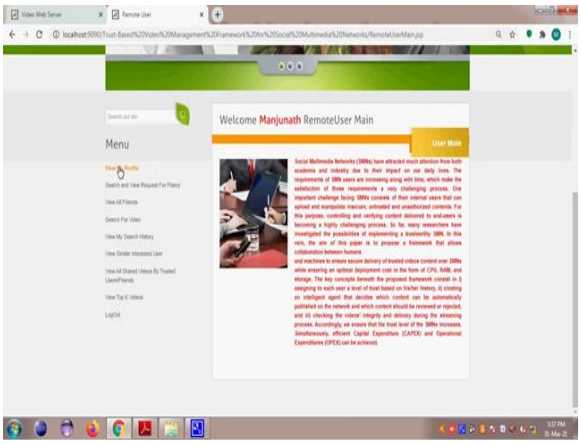

Fig3: - home page Remote User

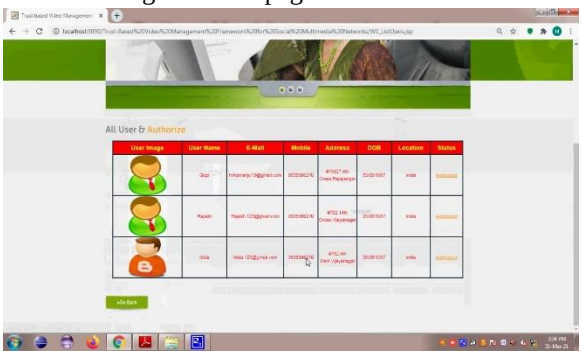

Fig4: - Authoring REMOTE USERS FOR ACESSING THE VIDOES

Fig5: - UPLOADED VIDEO WITH VIDEO DESCRPTION

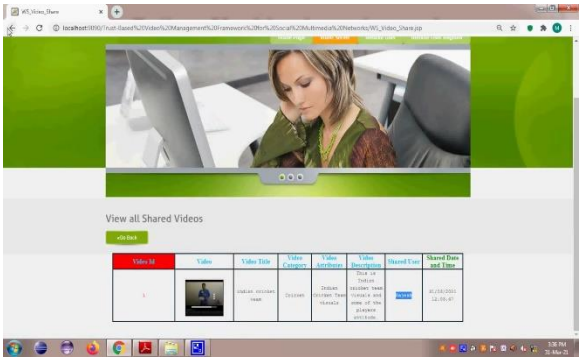

Fig6: - FILTERING THE DATA USING VIDOES META DATA AND PUBLISHING TO SERVER

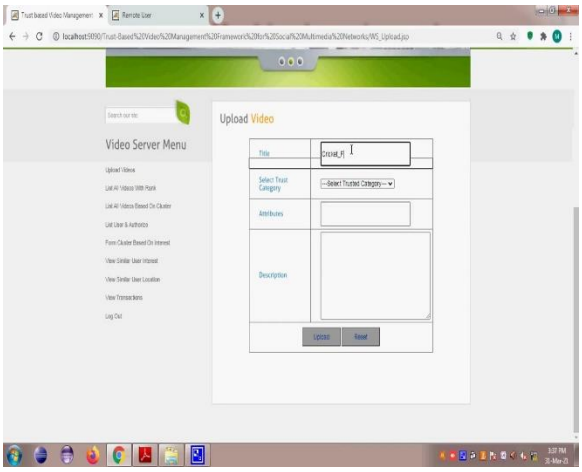

Fig7: - UPLOADING THE VIDOE WITH VIDOE DESCRPTIONS

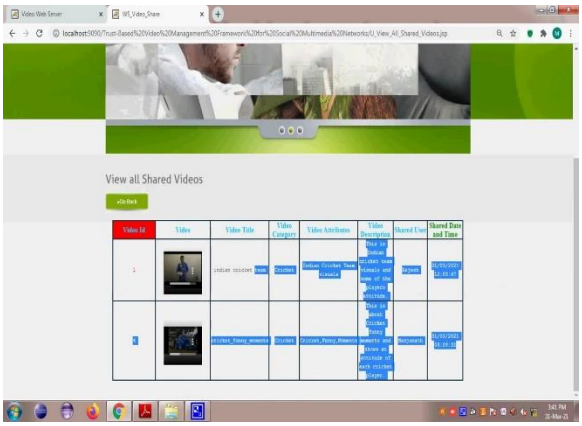

Fig8: - SHARED VIDOES DESCRPTION

VII.CONCLUSION AND FUTURE WORK

The growth of social multimedia networks is growing, and their services are becoming the most popular among Internet users. Users of these networks create and share a wide variety of data. Film, records, text, and photographs are among them. Unfortunately, some users have the ability to upload vulnerable, untrusted, and unauthorized material. As a consequence, a reliable method for monitoring and verifying the content that is exchanged is needed. We focused on how to ensure that users only upload safe, trusted, and approved videos to social multimedia networks in this research. As a result, we proposed a holistic system that considers a number of factors in assigning trust values to users and content, as well as securing video streaming in the process. The proposed architecture was developed with the intention of maximizing CPU, RAM, and storage resources while

minimizing resource consumption. Furthermore, we proposed a video uploading decision-making module that takes into account users' previous actions in order to make the best decisions on whether to accept or reject video uploads. These decisions are made with the aid of an infinite discrete Markov decision process (DMDP). This module will also determine if the contents should be analyzed or submitted to external reviewers before being published, or whether they should be excluded from being published. The simulation results show that the proposed algorithm is successful in terms of allowing good content to be published while preventing bad content from being published. Furthermore, the simulation results show that the proposed algorithms are effective in terms of reducing the computational expense.

REFERENCES

[1] L. Gao, H. Ling, X. Fan, J. Chen, Q. Yin, and L. Wang, "A popularity- driven 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 video- on-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.

[26] T. DuBois, J. Golbeck, and A. Srinivasan, "Predicting trust and distrust in social networks," in 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing, Oct 2011, pp. 418–424.

[27] K. Zolfaghar and A. Aghaie, "Mining trust and distrust relationships in social web applications," in Proceedings of the 2010 IEEE 6th International Conference on Intelligent Computer Communication and Processing, Aug 2010, pp. 73–80.

[28] X. Wang, Z. Xu, X. Xia, and C. Mao, "Computing user similarity by combining simrank++ and cosine similarities to improve collaborative filtering," in 2017 14th Web Information Systems and Applications Conference (WISA), Nov 2017, pp. 205–210.

[29] T. DuBois, J. Golbeck, and A. Srinivasan, "Rigorous probabilistic trust- inference with applications to clustering," in 2009 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology, vol. 1, Sept 2009, pp. 655–658.

[30] L. Cao and Y. Jiang, "An effective background reconstruction method for video objects detection," in 2012 Third International Conference on Networking and Distributed Computing, Oct 2012, pp. 161–165.

[31] B. Lu, S. Zhu, X. Ju, and L. Chen, "Adaptive codebook modeling based multiple objects detection," in 2018 Chinese Control and Decision Conference (CCDC), June 2018, pp. 2471–2475.

[32] F. Jabloncik, L. Hargas, D. Koniar, J. Volak, and Z. Loncova, "Dynamic objects detection of the respiratory epithelium based on image analysis," in 2018 ELEKTRO, May 2018, pp. 1–5.

[33] I. Agriomallos, S. Doltsinis, I. Mitsioni, and Z. Doulgeri, "Slippage detection generalizing to grasping of unknown objects using machine learning with novel features," IEEE Robotics and Automation Letters, vol. 3, no. 2, pp. 942–948, April 2018.

[34] S. Oh, M. Kim, D. Kim, M. Jeong, and M. Lee, "Investigation on performance and energy efficiency of cnn-based object detection on embedded device," in 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT), Aug 2017, pp. 1–4.

[35] B. E. Mada, M. Bagaa, and T. Taleb, "Efficient transcoding and streaming mechanism in multiple

cloud domains," in GLOBECOM 2017- 2017 IEEE Global Communications Conference, Dec 2017, pp. 1–6.

[36] M. L. Puterman, Markov decision processes: discrete stochastic dynamic programming. John Wiley & Sons, 2014.

[37] Markov Decision Processes: Discrete Stochastic Dynamic Programming, 1st ed. New York, NY, USA: John Wiley & Sons, Inc., 1994.