

# Social Multimedia Networks Behaviour Model & Architecture

L. K. Pulasthi Dhananjaya Gunawardhana  
Department of IT, School of Science and  
Engineering Malaysia University of Science and  
Technology (MUST) Kelana Jaya, PJ, Selangor,  
Malaysia

Professor Sellappan Palaniappan  
Head of Information Technology and  
Telecommunication Department,  
School of Science and Engineering Malaysia  
University of Science and Technology (MUST)  
Kelana Jaya, PJ, Selangor, Malaysia

**Abstract** - People constantly use social multimedia networks to communicate with one another, with users mostly sharing data, such as photos and videos. We examine the motivations that drive colluders to form alliances over social networking platforms and determine how these groups create coalitions to advance their interests. We also investigate the network architectures that underlie social multimedia networks and how these platforms circulate. Such architectures are connected to different protocols, including WebID, Semantic Pingback and PubSubHubbub, to form a logical semantic circulating social multimedia network that delivers a centralised social network structure.

**Key Words**-Social Multimedia Network; Social Media; Multimedia; Colluder; Peer-to-peer Network; Network Architecture; WebID; Semantic Pingback

## I. INTRODUCTION

Blogs and various other social media networking platforms currently serve as primary media channels for individuals who use the Internet on a daily basis. Today's media environment is characterised by the ubiquity of capture devices, such as phones and digital cameras. Such ubiquity has transformed the Internet into a channel for the delivery of tremendous volumes of multimedia content. Well-known social networking websites, such as Facebook, Blogger, LinkedIn, as well as content-sharing platforms, such as YouTube and Twitter, have established politically driven programs designed to facilitate content creation and sharing, thereby enabling people to easily accumulate large groups of friends. The combination of multimedia and social media has resulted in what may be called 'social multimedia'—innovations that support new ways of user interaction. Social multimedia provide an additional perspective from which the multimedia context can be understood. For example, several rounds of pausing and playing of a single YouTube video by a group of people render this particular video the most interesting content on the platform. Lazer et al. state that social multimedia are powerful tools that can potentially change how we

communicate and cooperate with one other [1]. Technology has rapidly developed in the past few years. The development of social media applications has considerably motivated the formulation of a computer-related hypothesis that serves as basis for evaluating and managing social behaviours and organisational characteristics. The findings from such investigations can then guide the production of smart software programmes. A problem that emerged from these innovations, however, is that the dominance of social multimedia has given rise to competition with social computing given that the latter is associated with the engagement in social activities and the interaction with multimedia that are also enabled by social computing. This issue requires precise discussion in media studies. Researchers continue to pursue subjects related to multimedia but are also confronted with the challenges of probing into the contexts that surround social networking technologies, such as social multimedia networks. Understanding social multimedia is expected to advance improvements to the social media applications currently available in the market. The term 'social multimedia' should be used to signify the importance such as like reflect the integration required to accurately explain the social multimedia phenomenon and its effects of the integrative research and applications that are presently available in the domains of social sciences and multimedia.

Accordingly, this paper discusses the procedures necessary to develop systematic multimedia social networks and the manner by which these technologies are secured. In this work, we use the term "multimedia social networks" to refer to the effects of social networking frameworks to identify user misbehaviours and examine system performance. In our discussion of the different frameworks used in various social media platforms, we assume that a central network plays a key role of running the social multimedia network. Identifying this role is expected to facilitate the identification of user misbehaviours. As a principal component of multiuser collusion, collaborator dynamics is

explored as a means of understanding the proliferation of such behaviour. We propose significant guidelines for counteracting such collusion through a fingerprinting system. Delving into this issue from the perspective of human behaviour necessitates conducting a case study on misbehaviour detection and fingerprint-based identification. This paper also discusses the architectures that underlie social multimedia networks and the circulation of social networks on the basis of semantic technologies and prevalent centralised social networks. Finally, we identify relevant approaches to developing social multimedia networks and the advantages provided by such innovations, as well as discuss matters such as the security of user data of longevity of these sites and their reliability.

## II. CHARACTERISTICS OF SOCIAL MULTIMEDIA

Mor defines social multimedia as ‘an online source of multimedia resources that fosters an environment of significant individual participation and that promotes community curtain, discussion and re-use of content’ [2]. The author also indicates social multimedia as having the following characteristics:

- Interaction amongst multimedia. Multimedia applications are developed from a combination of several related but not necessarily time-based media technologies. This characteristic is exemplified by a user who uploads a video or an image with several keywords or hashtags on YouTube or Twitter to elicit a specific spectator response.
- Social interaction with multimedia. This characteristic revolves around the relationships of people with selected groups. It also pertains to the use of multimedia as an avenue where connections are formed and data are transmitted. Blogs with images or videos and social networks, such as Twitter and Facebook, reflect the social interaction component of social multimedia.
- Social interaction integrated with multimedia. Most multimedia tools and interactions are considerably represented in social multimedia. CCTVs or surveillance cameras, YouTube channels and online TV are some of the key avenues in which this characteristic is manifested. The integration offers users moment-by-moment videos over extended periods.

In addition to these characteristics, a few other features enabled by the social media context have been incorporated into multimedia tools and

applications. Awareness of these features enables the analysis of social multimedia content. The context extension of capacity in multimedia research has been a relatively extensive field and has been broadly discussed in the past few years.

## III. SOCIAL MULTIMEDIA NETWORKS

Fellowship in a social network is a theoretical sense that the network’s users are associated with one another through several different relationships, such as friendship, personal business, conflict and financial exchange. People adhere to many procedures that articulate their relationships with parties of all types; these connections range from the interpersonal to the international domain and across numerous fields, including sociology, politics, economy and IT. In multimedia social networks, users are willing to form a network framework that dynamically transforms to enable the exchange of data and other resources. The specific manner by which a user collaborates, however, is uncertain if a key system fully compels a user to engage in this behaviour. Research reveals that Napster and Gnutella are freely used by most of their users but that around 20% of Gnutella users do not share any files with other individuals [3]. As indicated by Buragohain and his colleague, the success of social multimedia networks depends on their effectiveness at providing satisfactory services; the development process for such network should involve considerable evaluation because this step enables developers to incorporate features that facilitate usage [4]. The authors also assert that most design arrangements can successfully encourage collaboration but that tamper-proof hardware intended to track interactions is necessary. Another requirement in designing social multimedia networks is a set of motivational measures for using reputation-based methods that distinguish users; for this purpose, the difference facility model is assumed to provide good services to users who contribute more substantially to a network [4].

Users receive payoffs from using social multimedia networks by obtaining access to the resources shared by their peers. Most users are driven by the desire to maximise the rewards that they acquire from contributing to social multimedia networks. Many types of users patronise social multimedia networks. Coherent users are individuals who readily share their resources if collaboration with others means an increase in rewards. Selfish users are upfront about their motives when they are exchanging information with other individuals. They differ from coherent users in that they desire to acquire others’ resources without providing anything in exchange. Selfish users even deceive others during the negotiation process just to increase the rewards that they obtain. To analyse human dynamics in social multimedia networks that comprise selfish and malicious users, administrators should examine the strategies used by these users to deceive a social organisation or group. Another requirement is to

requirement is to develop a monitoring application that identifies user misbehaviours. This goal is challenging because an effective application is one that can identify intentional misbehaviours even from selfish users.

Given that social multimedia networks are underlain by different frameworks, developers can use many different techniques for developing anti-deception policies. A number of networks are equipped with an integrated arrangement wherein no user is accorded trust. The drawback of integrated servers is that they do not deliver effective regulations for imposing user collaboration; they can only aid the monitoring of user behaviour. Lua and his colleague explain that social multimedia networks can serve as a central billing unit for payments because they can monitor transactions and detect user misbehaviours. The authors also reveal that most of the social multimedia networks consist of a circulated structure that allows users to use the same network facilities; examples include Gnutella and Chord [5]. In this type of social multimedia network, users are required to monitor the conduct of other users and recognise their own misbehaviours.

Social multimedia networks are composed of numerous users who espouse various objectives. In this regard, the analysis of user dynamics is a significant concern because such examination promotes user documentation and consequently simplifies the implementation of misbehaviour monitoring applications. It also provides a useful procedure for designing anti-deception measures and policies. Analysing user dynamics and designing anti-deception measures/policies are essential to improving the performance of a system and reducing the problems caused by mischievous users.

#### IV. BEHAVIOURAL DYNAMICS IN COLLUDER SOCIAL MULTIMEDIA NETWORKS

Users of social multimedia networks can augment their assets by developing their own resources and collaborating with other users. All users are driven by the purpose of increasing their rewards, but these individuals differ in terms of their specific goals. Determining these dissimilarities necessitates examining users' approaches to achieving a sense of fairness. Colluders typically share rewards from illegal usage of video content; they often contend with the risk of being identified by a fingerprint scanner. In collusion exercises, invaders attempt to influence a network's multimedia fingerprint system to be able to use content illegally. Colluders always operate under the principle of balancing risks and rewards. They reduce the risk of identification by enlisting help from other users. To ensure successful collusion, colluders decide on how they will distribute risk amongst themselves by organising a collusion

exercise in accordance with a multimedia signal. Colluders who manipulate multimedia fingerprint systems also need a social network.

Despite this apparent cooperation, most colluders prefer risk decisions that rule in their favour rather than benefit other parties. When they address their goals, colluders normally apply the principle of fair collusion, in which the risk of being identified is distributed equally amongst the members of their group. The value of restructured multimedia content is time sensitive, but most people are willing to work with a colluder who can ensure the early release of content. This willingness encourages colluders to decide on a strategy for allocating rewards, making them vulnerable to identification. To achieve fairness, all colluders need to present correct information about their fingerprint copies. This requirement guarantees successful collusion attacks.

When colluders obtain fingerprint copies of the same resolution, including the same regular weights, they moderate the dynamic characteristics of each fingerprint at the same ratio. This reduction helps them confirm the risk with which invaders have to contend. However, if colluders acquire fingerprint copies of different resolutions, collusion becomes a complicated task. The problem that arises from this situation is the need to divide risk equally amongst all colluders. The situation becomes even more complicated when colluders are required to produce a colluded copy in high resolution. Additionally, if colluders obtain fingerprint copies of different resolutions because of an error from a network, these individuals encounter difficulties in ensuring fairness for the members of their groups. When collusion fails to provide the agreed-upon fingerprint, agreements regarding the risk borne by invaders will also be ineffective because colluders cannot achieve desired outcomes. A probable solution is depicted in Figure 1.

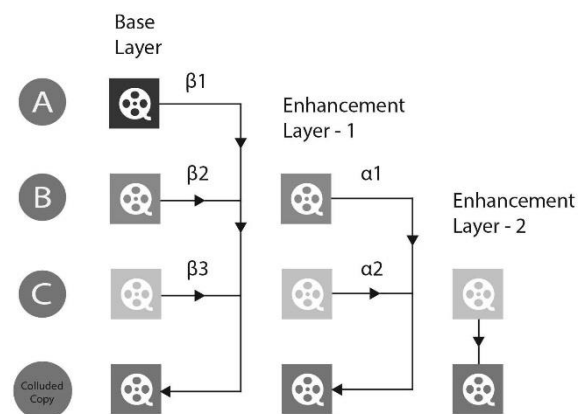


Figure 1

Figure 1 shows three fingerprint copies with weights  $\beta_1$ ,  $\beta_2$  and  $\beta_3$ . An enhancement layer includes colluded copies labelled as 'B' and 'C', which are assigned weights of  $\alpha_1$  and  $\alpha_2$ , respectively. The colluder's copy is the same as

Carl's copy; an enhancement copy also exists. To achieve fairness in collusion, A, B and C are informed about collusion parameters that ensure they will have to contend with the same possibility of being identified. If the colluders obtain fingerprint copies with different resolutions, they will carry out two-stage collusion (Figure 1) to bear a similar extent of risk and achieve fairness. They will allow this situation to happen in intergroup collusion to come to a settlement with colluders who obtain fingerprint copies of the same resolution. Under this backdrop, colluders will likely be identified. The colluders will apprise the others of this situation during the intergroup collusion to confirm that colluders who obtain copies of different resolutions bear the same risk as they do. Simultaneously, they will incorporate this shared risk into the intragroup collusion; thus, the colluders conspire with the invaders of a similar group. These measures result in fewer copies with different resolutions and the same weights. This intragroup collusion confirms that colluders who acquire fingerprint copies of the same resolution contend with the same possibility of being identified.

#### V. SOCIAL MULTIMEDIA NETWORKS WITH PEER-TO-PEER CAPABILITY

Social multimedia networks are widespread. Users are guaranteed a certain programme and are rarely motivated to switch to another social web application if they want to maintain their connections. Interoperability amongst platforms is a basic feature and mostly limited to certain APIs. To keep data updated in various platforms, users are required to adjust data that are to be transmitted to different platforms; otherwise, information is lost. Meanwhile, because fewer social networks than social multimedia networks exist, the circulated patterns of the former may be disregarded over the Internet. Peer-to-peer networks are distributed frameworks that comprise network topology nodes designed for resource sharing. Content sharing for an outstanding application equipped with the capacity of peer-to-peer systems is developed on the basis of a design structure that enables sharing of multimedia files. Shirky states that 'peer to peer is the class of applications that takes advantages of resources-storage, cycle's content, human presence-available at the edges of the internet' [7].

The most reputable and extensively used peer-to-peer file sharing applications are Gnutella, BitTorrent and LimeWire. Websites, such as WYAN and LinkedIn, require users' Facebook or other popular social network accounts for peer-to-peer networking with TCP. The most commonly adopted method of using peer-to-peer networks is joining popular social networks that incorporate users' social network accounts. Signing up for a LinkedIn account, for instance, necessitates a Facebook or Twitter account. This method enables users to maintain their Facebook connections and share multimedia content even as they maintain

another social network account. The presence of this feature is the initial measure of a peer-to-peer network's lifecycle because this means overlap with other networks and setups based on the aforementioned method. A user is then afforded access to their social network friends via this peer-to-peer network method. Platforms grounded on peer-to-peer networks are also supported by TCP given that most network applications are designed for sharing files and information, including, images, text files and videos. TCP therefore helps improve the consistency of a social networking site.

A huge gap regarding the availability of social network applications and usage exists. This gap is addressed with the help of a high-speed Internet connection because rapid connectivity enables on-demand data transmission and connection to web applications. Most social network applications are functional with several small-scale users connected to a network. Using popular social network applications exposes us to the advantages of using a peer-to-peer network system. These advantages are as follows:

- **Privacy.** A distributed semantic social network (DSSN) helps users set up their own DSSN nodes or select a DSSN node provider as they wish. However, a DSSN should implement stringent privacy procedures to secure user privacy during access to social networks. The developers of large-scale social networking sites, such as Facebook, Google and Twitter, created their own privacy strategies to attract users to their networks. This strategy builds up the trustworthiness of a platform.
- **Extensibility.** Artefacts that represent social network assets (e.g. WebIDs and data objects) are not confined to a certain structure, thereby allowing for keeping pace with user needs. Even though extensibility is a fundamental component of network systems, a core social network setting can exclude certain extensions for commercial purposes, thus constraining the freedom of users.
- **Liberty in interaction.** The Arab Spring phenomenon confirms that social networking helps individuals organise protests and voice their own perspectives. In this situation, social networks critically contribute to achieving civil rights and freedom.
- **Data copyright.** Users can protect and control the use of their data. They can implement ownership protocols and exercise their right to use a certain social network. DSSNs help users implement data authorising options as they wish.

Thus far, the discussion has mostly revolved around the technological elements of DSSNs. The dialectal features of network information are enabled by a WebID profile. This WebID technique enables individuals to use a WebID profile for verification purposes. Dialectal features enable an initial link between users and a social network by implementing techniques for sharing the resources available in the network. Social network-centred support services issue prompt notifications for certain information, such as changes to WebID profiles and action streams, through other users in a social network. Combining these principles and techniques advances the delivery of elements that are essential to comprehending the circulation of social networks and allows the incorporation of the fundamental features that characterise centralised social network settings.

## VI. ARCHITECTURES OF SOCIAL MULTIMEDIA NETWORKS

This section begins with a discussion of design principles, followed by a brief explanation of four architectural layers, namely, the data, protocol, service and application layers. A network architecture composed of these layers was developed by Tramp et al. in 2012. This section also describes how this social network architecture works. Figure 2 illustrates the architectures commonly used in social networks [9].

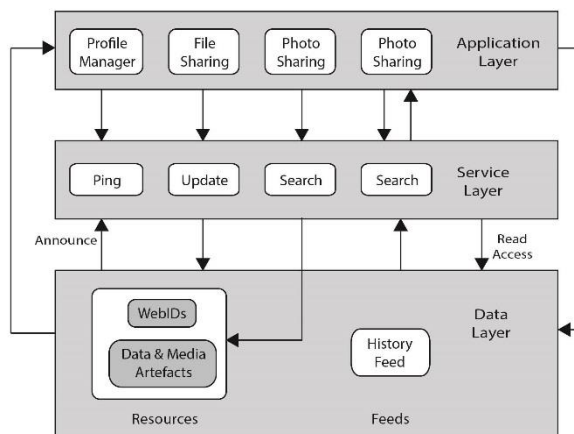


Figure 2 [9]

### A. Design Principles

Three significant principles are espoused in network theory. An important requirement in the study of social networks is determining how these principles are applied in social multimedia networks. The principles are discussed as follows.

#### Linked Data

Berners-Lee indicates that the core procedure for distributing, recovering and incorporating data is using linked data principles [10], which are

advanced by flexibility and the circulation of information and services for websites. The final outcomes of specifying the nature of a given architecture are consistency and the independence to communicate and ensure information security through design.

#### Service Decoupling

This principle pertains to how a user's data are decoupled from network features and applications. It guarantees user selection of an option amongst various services and applications and facilitates additional circulated normalities to social networks, thereby compelling the circulation of the same information across linked data. Additionally, service decoupling supports DSSN users as they classify the data that they share with other users. They are licensed to use data on services and applications from other individuals. These data are independently acquired by users through facilities that they can access but do not possess.

#### Protocol Simplification

The key task of social networking protocols is to interact with RDF augmentations that occur between DSSN nodes and not to execute a certain work flow. Adherence to this task certifies the flexibility of a data model and keeps an entire architecture clean and consistent.

### B. Data Layer

A data layer consists of two key data frameworks, namely, resources and feeds.

#### Resources

For easy discussion, resources can be broken down into three subtopics that are primarily a component of DSSNs. These subtopics are WebID, data artefact and media artefact.

**WebID** – WebID is used principally to identify a website for users. As the motivation of this protocol is straightforwardness, the demands for a WebID profile are nominal. WebID profiles are embedded with an RDF that can identify its vendor. Brickley and Miller indicate that information about a vendor can be obtained through the use of appropriate terminologies because this approach ensures that necessary standards can be continued [12].

**Data Artefact** – Data artefacts are resources that are published and conferred to linked data. As Breslin et al. explain, these artefacts contain information on all user activities, such as sharing posts, comments, tags and activity feeds. These artefacts are created with social network applications [13].

**Media Artefact** – Media artefacts are created by services and specific social network applications.

They are characterised by binary data sections, which can be deciphered with a specific codec application. The sections also consist of metadata that define media artefacts. Audio, video, image files and other document types that are viewable over social media networks can be categorised as media artefacts.

### *Feeds*

Feeds are used to characterise systematic information in a readable manner. They are used mainly for web-based activities. Their essential parts function whilst connecting to the PubSubHubbub protocol, thereby enabling real-time interaction amongst various services. Two types of feeds are the activity and history feeds.

**Activity Feed** – These designate the social multimedia network activities in which users currently engage. Activity feeds can be productive as tools that combine opinions on the actions executed in a social network. As to the DSSN architecture, each activity is produced via linked data. These data are linked to an entity that underlies certain activities. Most of the activities are equipped with a Pingback Server to bring consensus to get the feedbacks from the Pingbacks and therefore to twist the contents of the network among the artefacts.

**History Feed** – History feeds are associated with changes to the assets of individuals who published the assets. The variable in RDF resources for adding and deleting declarations are recorded in entries. A subscriber's social network application can be used to obtain information that maintains a particular copy of the original assets for persistent caching and inquiry. History feeds are particularly essential for linking the differences amongst WebID profiles.

### *C. Protocol Layer*

A protocol layer contains the WebID, Semantic Pingback and PubSubHubbub networking protocols. It supports two different interaction methods.

#### *WebID*

The purpose of a WebID is to establish a connection with an SSL client certificate in a safe manner. It therefore grants WebID-holding users permission to validate third-party websites with support for the WebID protocol. From a technical perspective, the WebID protocol integrates confirmation and confidence about the WebID method. A WebID is driven in into a certification number; X.509 is used with the subject alternative name extension. All the certificates that are recovered through the URI process comprise a confirmation key. Passing on particular data, this can be contested by retrieving the user that holds a precise WebID. Additionally, the WebID protocol

implements an approach that controls the operation of the social networks formed into WebIDs. This control is intended to regulate access to the confidential information and assets of other users. In circulated social networks, however, this procedure is not always applicable. In this case, an explanation is given for the WebID certification of a particular application. A user needs to create another certificate for presentation as a legal document that affords the user access to protected files. This certificate then allows the use of any tool to hack identities. This is not ideal solution from the perspective of protection. Resolving this problem requires the stringent implementation of the WebID protocol for access allocation. By allowing access to a proxy, a user may permit a specific proxy to facilitate access to protected data and resources. Unlike reliance on a party that applies its own certification, the proxy helps users validate access.

#### *Semantic Pingback*

Langridge and Hickson regard the Semantic Pingback layer as an expansion of Pingback technology. Semantic Pingback is one of the most successful technological infrastructures for social networks [14]. A layering method grounded in this infrastructure facilitates bi-directional connection amongst WebIDs, RDF assets and other linked websites. It alerts a user about cases wherein a connection is newly built. Semantic Pingback is based on the trivial RPC facility that provides the RDF documents or headers of websites assets written in HTML, which should be activated soon after assets are connected. The Semantic Pingback structure allows users and RDF content writers to obtain instant feedback once other users obtain related assets, thereby enabling social interactions. Semantic Pingback also allows the spontaneous circulation of backlinks by using a WebID profile as reference for a WebID that is located in a different area of a website. Accordingly, the relevance and reliability of a social network are guaranteed. Thereby, circulated WebID profiles, RDF assets and social websites are considerably more securely interlinked through the Semantic Pingback method than are conventional websites. Interpreting the effects of a network is one of the key components of understanding social networks. Semantic Pingback is compatible with descending conventional Pingback processes, thereby allowing the integration of links and the interlacing of a social network's assets with those of a DSSN.

#### *PubSubHubbub*

PubSubHubbub is a web-hook circulating protocol than can expand to RSS. RSS is activated for feed access that occasionally circulates through one generator to several subscribers. In the meantime, feed access cannot be define via RDF assets. However, this protocol uses atom feeds; that is, it generally uses atoms and delivers solid backup

to web developers. Similar to Semantic Pingback, PubSubHubbub is sceptical towards payload and can be used for all circulating linked networks.

#### *D. Service Layer*

A service layer centres on all the applications that operate as part of the DSSN context. Elements such as WebIDs can be equipped with different functions, including managing actions that run user data through other applications. For convenient explanation, service layers are subdivided into key services, namely, the Ping, Push and Search and Index services.

##### *Ping Service*

The Ping service runs to the endpoint through any incoming requests by using a user's assets. Initially, the service is used primarily with a WebID when users search for someone with whom they are acquainted and when discussions are conducted. For many available assets, a single ping is helpful in delivering the service through an application. The lowest system on which the Ping service runs is that for notification by email. With respect to a multiplex system, the service contacts an update service via a user and then transmits a notification.

##### *Push Service*

The Push service is normally used in social multimedia networks to circulate and synchronize assets. In the meantime, both activity and history feeds are usable with atoms, and the Push service for a DSSN is occasionally accepted over PubSubHubbub. Breslin et al. declare that equipping the assets of a social multimedia network with consistent activities necessitates incorporating OWL objects into the network because they are in the SIOC:feed link with the SIOC project dssn:activity feed and dssn:sync feed [13]. With regard to provided RDF assets, DSSN proxies are considered for the consistency of an HTTP header, activity feed and sync feed. These substitutes to OWL objects allow users to conveniently incorporate media artefacts into a network.

##### *Search and Index Service*

Two different frameworks are used for social multimedia networking architecture. Ding et al. state that Search and Index services are used primarily to search public assets. For this purpose, popular semantic search engines, such as Swoogle, are used [15]. These services always use sycophants to maintain updated assets and data, as well as functional applications that are delivered to users. With respect to network architecture, Search and Index services constantly use search contacts and related artefacts to execute the search function. Users can also use these services as a typical web search engine.

A helpful approach to understanding Search and Index services is emphasising the effects of private search services on social networks. The services enable considerably efficient caching of assets and allows access to both private and public data. Private searching is accessible to all users who use a given application in a network and operates on behalf of the users. The fundamental assets for a private search service and its index is helpful in retrieving all push notifications that are transmitted by users through feeds. As previously stated, private search services are always suitable for use with an application, but it must be enabled with the WebID protocol. The use of the protocol enables acceptance of requests only by users.

#### *E. Application Layer*

This section describes how social multimedia web applications are developed and adjusted to accommodate all users' assets. Through this network architecture, individuals can use an application by accessing the reliable services linked to WebID. Because access is granted exclusively to a user, control over his/her data and assets is also restricted to this individual. When users create an account, they are required to enter their own WebIDs in the first login to access to a social multimedia application. The application then examines the WebIDs, provides confidential services and adds metadata for users. After this, users can upload video and image files to the desired application. The social multimedia application creates a new folder for the uploaded assets and activates a stream for these assets. Application layers are equipped with the pingback service, thereby enabling backlinking and commenting on images, videos or any other posts. All comments can be received from any of the users of a platform. When another user responds to someone's post, image or video, the data artefact produces a namespace by using the application and sending a ping request to the posting user's pingback service.

## VII. CONCLUSION

The development of social multimedia networks has modernised the manner by which content is circulated and interaction tasks are completed. This paper comprehensively analysed these networks, the structure that underlies them and the methods by which they are developed. Current technological use in relation to the human dynamics behind the use of social multimedia network was also discussed. The other issues presented in this paper are the effects of network security based on signal processing insights, current security frameworks and the analysis of such frameworks. Another significant issue that we described is collusion in multimedia fingerprinting. We defined social multimedia architectures and distributed social multimedia networks on the basis of semantic technologies, as well as presented a summary of these matters. We

likewise described the centralised system that is prevalently used in social multimedia networks. Our analysis reveals that social connections amongst users elevate exchange, sharing and data delivery, thereby also improving service and application provision. Finally, a literature review was conducted to discuss key concepts of social multimedia networking systems, pressing problems related to social multimedia networks and development approaches. This paper contributes to the literature by outlining several directions that technology may take in the future.

#### Acknowledgement

I would like to take express my gratitude to everyone who supported and guided me especially my PhD research supervisor, Professor Dr P. Sellappan.

#### Authors Profile



I, Pulasthi Gunawardhana currently reading PhD in Informatics at Malaysia University of Science and Technology, Malaysia. I'm member of IEEE Computing Society. I have written several journal articles related to Multimedia since 2014.

#### Reference

- [1] Lazer, D., Sandy, Alex., Pentland, Adamic, L., Aral, S., Barabasi, Albert Laszlo., Brewer, D., Christakis, N., Fowler, Albert Laszlo., Gutmann, M., Jebara, T., King, G., Macy, Michael., Roy, D., Alstyne, Marshall Van. Computational Social Science Social Science, vol. 323. 6 Feb, 2009, pp. 7-723.
- [2] Naaman, Mor. Social Multimedia: highlighting opportunities for search and mining of multimedia data in social media application. 2010, Springer, US.
- [3] Saroiu, S., Gummadi, G. P., and Gribble, S. A measurement study of peer-to-peer file sharing systems. SPIE Proceedings. Multimedia Computing and Networking, 4673(156) December 2002, USA
- [4] Buragohain, C., Agrawal, D., and Sur, S. A game theoretic framework for incentives in P2P systems, Peer-to-Peer Computing, 2003. (P2P 2003). Proceedings. Third International Conference, Sept 2003, (48-56)
- [5] Lua, E., Crowcroft, J., Pias, M., Sharma, R., and Lim, S. A survey and comparison of Peer-to-Peer overlay network schemes. IEEE Communication, USA. Surveys Tutorial, 7(2),
- [6] Vicky Zhao, H. and Ray Liu, K. J. Behavior Modelling for Multimedia Networks. IEEE Signal Processing Magazine, USA. January, 2009
- [7] Shirky, Clay. What Is P2P and What Isn't. Internet and teaches at NYU's Interactive Telecommunications Program. O'Reilly Network. November, 2000.
- [8] Nipendra Kayastha, Dusit Niyato, Ping Wang, and Ekram Hossain. Applications, Architectures, and Protocol Design Issues for Mobile Social Networks: A Survey, Proceedings of the IEEE. Vol. 99, No. 12, Dec.
- [9] Tramp, Sebastian., Frischmuth, Philipp., Ermilov, Timofey, Shekarpour, Saeedeh., and Auer, Sören. An Architecture of a Distributed Semantic Social Network. IOS Press. Semantic Web. 2012
- [10] Berners-Lee, T. Linked Data: Principles and State of the Art-Design Issues, 7th International World Wide Web Conference W3C Track. Massachusetts Institute of Technology, USA, July 2006.
- [11] Krohn, M., Yip, A., Brodsky, M., Morris, R., and Walfish, M. A World Wide Web Without Walls. In 6th ACM Workshop on Hot Topics in Networking (Hotnets), Atlanta, GA, USA, November 2007.
- [12] Brickley, D., and Miller, L. FOAF Vocabulary Specification. Namespace Document, FOAF Project, 2004.
- [13] Breslin, J. G., Decker, S., Harth, A., and Bojars, U. SIOC: an approach to connect web-based communities. International Journal of Web Based Communities, 2(2):133-142, 2006.
- [14] Langridge, S. and Hickson, I. Pingback 1.0. Technical Report, personal document, 2002.
- [15] Ding, L., Finin, T. W., Joshi, A., Pan, R., Cost, R. S., Peng, Y., Reddivari, P., Doshi, V., and Sachs, J. Swoogle: a search and metadata engine for the semantic web. In Proceedings of the 2004 ACMCIKM International Conference on Information and Knowledge Management, Washington, DC, USA, November 8-13, 2004, pages 652-659, 2004.
- [16] Zhao, Vicky., Lin, Member, Sabrina. W., and Liu, Ray. R. J. Cooperation and Coalition in Multimedia Fingerprinting Colluder Social Networks. IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 14, NO.3, JUNE 2012.