"TRUST-BASED VIDEO MANAGEMENT FRAMEWORK FOR SOCIAL MULTIMEDIA NETWORKS"

Mohammed Dastagir[1], Syed Adnan Hussain[2], Abdul Sattar Danish[3], Mohd Hasan[4], Abdul Ahad Afroz[5]

[1,2,3,4]B. E Student, Department of IT, ISL College of Engineering, India.

[5]Assistant Professor, Department of IT, ISL College of Engineering, Hyderabad, India.

ABSTRACT : This project's objective is to develop a framework that enables people and machines to work together in order to guarantee the safe distribution of trusted video content via short message networks (SMNs). On the basis of the proposed framework, the key concepts include the following: i) the assignment of a level of trust to each user based on his or her history; ii) the creation of an intelligent agent that decides which content can be automatically published on the network and which content should be reviewed or rejected; and iii) the checking of the videos' integrity and delivery while they are being streamed. Therefore, we make it a point to guarantee that the degree of confidence in the SMNs continues to rise. At the same time, maximize the effectiveness of capitalization.

INTRODUCTION

The Internet's fast progress has led to the emergence of several online apps and social multimedia networks (SMNs), including Facebook, Twitter, and Google. These platforms have fundamentally revolutionized worldwide connectedness. These platforms have optimized communication, enabling users to easily communicate ideas, views, and numerous types of social information. Furthermore, they have enabled companies and organizations to expand their reach and interact directly with consumers on a worldwide level. In addition to these social networks, platforms such as YouTube, Dailymotion, and Vimeo have made it easier for networked organizations to share a wide range of information, including text, photographs, and videos.

The development of the Internet and distributed systems has stimulated the creation of programs that provide video material on-demand (VOD) via peer-to-peer (P2P) networks. Video on demand (VOD) and live streaming systems are becoming more common in social media networks (SMNs). These systems provide a wide range of multimedia-focused services, including video conferencing, online meetings, massive open online courses (MOOCs), and applications in ehealth and e-teaching. These services have a global appeal, attracting millions of users and facilitating considerable engagement and exchange of material among participants. Nevertheless, the widespread creation of content by users in social media networks (SMNs) poses difficulties with the handling of data, ensuring security, and establishing trust. The vast amount of data produced by users and machines overwhelms networks and presents security vulnerabilities, creating challenges for service providers to efficiently monitor and control the material that flows through their platforms. Therefore, it is crucial to

guarantee the reliability of SMNs, which are defined by the qualities of certainty, validity, and security in the flow of data.

As a result, many trust models and reputation systems have been developed to reduce the dissemination of insecure data and foster trust among network entities. These models use user behavior to provide scores, facilitating informed decision-making and allowing the implementation of necessary measures to protect network integrity. When creating trust models, it is important to consider factors such as assessing user history, determining trust levels, promoting user participation, and assuring safe information delivery.

Although considerable efforts have been made, effectively preventing the upload of unsecure, untrusted, and illegal material continues to be a major difficulty. Current methods depend on user reporting to detect and deal with dangerous content. This research aims to fill this need by presenting a universal architecture for establishing a reliable social media network (SMN) that guarantees the safe transmission of trusted video content while reducing resource use. The framework utilizes user history and participation to make educated judgments about content analysis. It has modules for trust calculation, voting, incentives, secure video transmission, and video integrity verification. In addition, it incorporates modifications to the video player and a module for making decisions about uploading videos in order to improve the control of content quality. The framework intends to improve the security, integrity, and trustworthiness of SMNs, creating a safer and more dependable environment for both users and content providers.

PROBLEM STATEMENT:

"In the era of social media dominance, ensuring the secure delivery of trusted video content over Social Media Networks (SMNs) poses a significant challenge. The proliferation of unverified and potentially harmful content threatens the authenticity, integrity, and safety of users' experiences. Existing trust models and reputation systems, while valuable, often fall short in effectively mitigating the spread of unsecured data. Moreover, the dynamic nature of user behavior and content interaction demands a proactive approach to content moderation and enforcement of security measures. Therefore, there is a critical need for a comprehensive framework that leverages collaboration between humans and machines to enhance trust levels, automate content evaluation processes, and ensure the integrity and security of video content throughout its lifecycle on SMNs. Addressing this need is essential to foster a trustworthy social media environment conducive to healthy interaction and information exchange."

LITERATURE REVIEW

The paper titled "A popularity-driven video discovery scheme for the centralized P2P-VoD system" by Gao et al. explores a method for discovering videos in a centralized peer-to-peer video-on-demand system based on their popularity.

Gao and colleagues provide a new method for speeding up the process of finding videos in a centralized Peer-to-

Peer Video on Demand (P2P-VoD) system. Their approach entails the implementation of a popularity-driven storage model, where films are arranged in a binary tree structure according to their popularity rankings. The authors validate their strategy experimentally, demonstrating its usefulness in lowering video finding latency and maximizing resource consumption in the system.

The paper titled "Social VOD: A social feature-based P2P system" by Chang and Wu:
Chang and Wu propose the innovative idea of "Social VOD," which involves a Peer-to-Peer (P2P) system that is based on users' social connections and commonalities in video channels. Their suggested system design implements a hierarchical overlay in which subscribers belonging to the same channel create a low-level overlay. This novel strategy seeks to tackle issues associated with the delay in video processing by using social connections and channel affinity to improve the effectiveness of distributing and consuming material.

The paper titled "Neighbors-buffering-based video on-demand architecture" by Taleb, Kato, and Nemoto:
Taleb, Kato, and Nemoto provide a sophisticated framework for Video on Demand (VoD) services in a multicast setting, focusing on a neighbors-buffering method. Their technique improves scalability and resource efficiency in providing on-demand video streams by using surrounding nodes to store video material. The authors' study provides valuable insights on how to address scalability difficulties that are often encountered in VoD systems running in multicast contexts.

The article titled "System and method for creating multimedia content channel customized for social network" by Taleb & Taleb:
Taleb and Taleb propose a technique designed to improve the user experience on social networks by creating personalized multimedia content channels. Their technology autonomously arranges and oversees the timing of material channels, specifically customized to suit the tastes of each individual user. Although their technique effectively deals with auto-playback problems and improves content distribution on social networks, it does not directly address security challenges associated with video material.

The paper titled "Enabling trustworthy service evaluation in service-oriented mobile social networks" by Liang, Lin, and She:
Liang, Lin, and She aim to improve the reliability of service assessment in mobile social networks by introducing the bTSE and SrTSE methodologies. Their study highlights the significance of countering service review assaults, and their offered techniques strive to efficiently withstand such attacks, guaranteeing the trustworthiness and dependability of service reviews. Although their research deals with security issues in mobile social networks, it does not explicitly concentrate on the specific material included inside videos.

SYSTEM ARCHITECTURE

A system architecture or systems architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system. Organized in a way that supports reasoning about the structures and behaviors of the system.
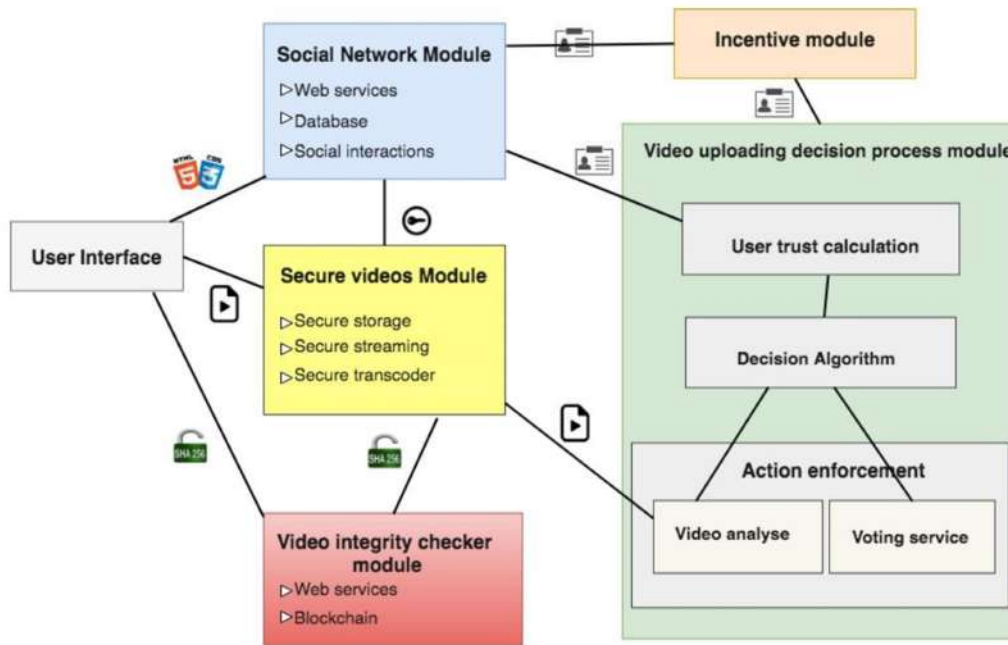
Figure 5. 1 System Architecture

3-Tier Architecture:

The three-tier software architecture (a three-layer architecture) emerged in the 1990s to overcome the limitations of the two-tier architecture. The third tier (middle tier server) is between the user interface (client) and the data management (server) components. This middle tier provides process management where business logic and rules are executed and can accommodate hundreds of users (as compared to only 100 users with the two tier architecture) by providing functions such as queuing, application execution, and database staging.

The three tier architecture is used when an effective distributed client/server design is needed that provides (when compared to the two tier) increased performance, flexibility, maintainability, reusability, and scalability, while hiding the complexity of distributed processing from the user. These characteristics have made three layer architectures a popular choice for Internet applications and net-centric information systems.

**INPUT & OUTPUT REPRESENTATION**

INPUT DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and

keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

SYSTEM TESTING

Testing is the debugging program is one of the most critical aspects of the computer programming triggers, without programming that works, the system would never produce an output of which it was designed. Testing is best performed when user development is asked to assist in identifying all errors and bugs. The sample data are used for testing. It is not quantity but quality of the data used the matters of testing. Testing is aimed at ensuring that the system was accurately an efficiently before live operation commands.

RESULT
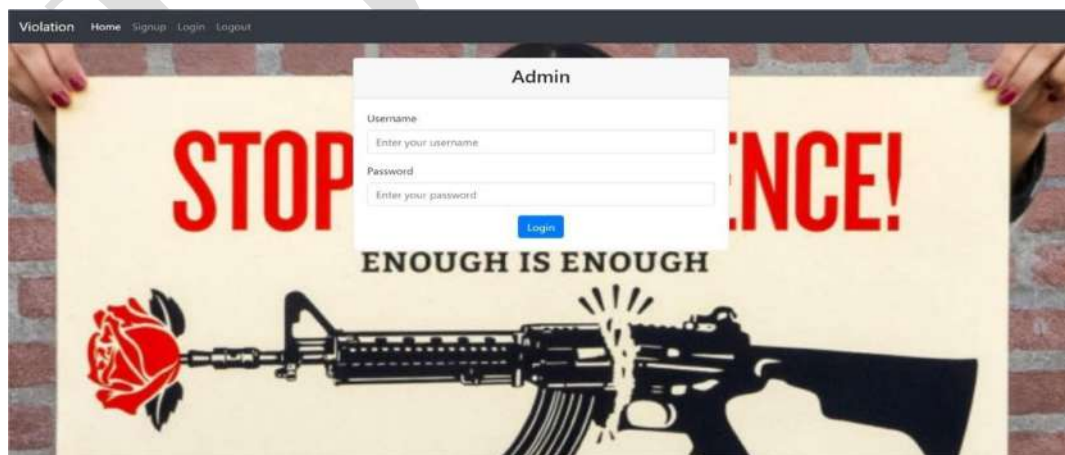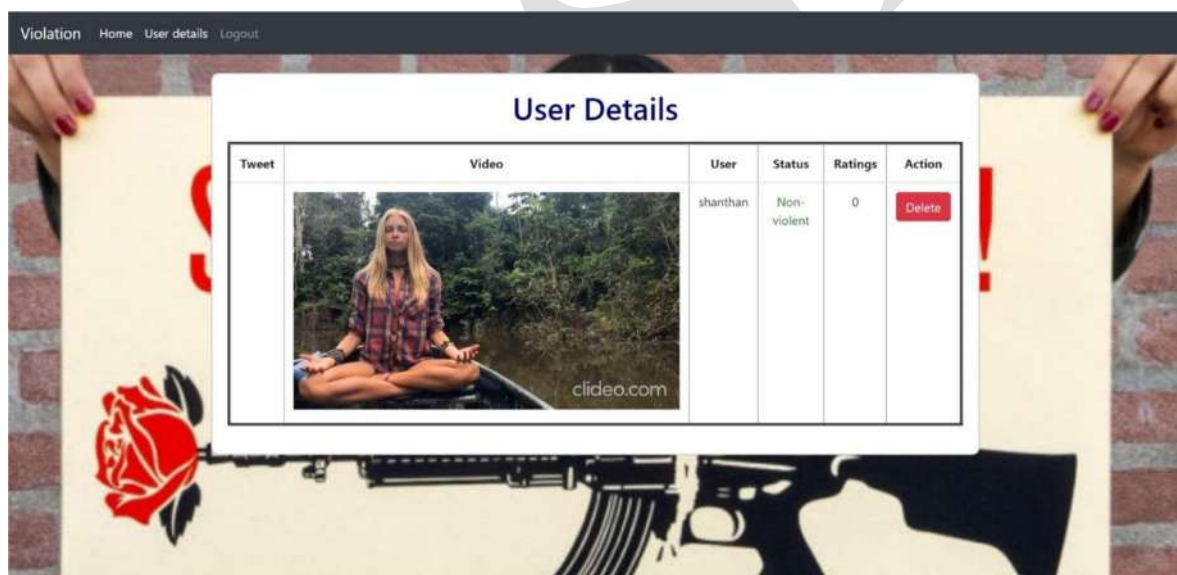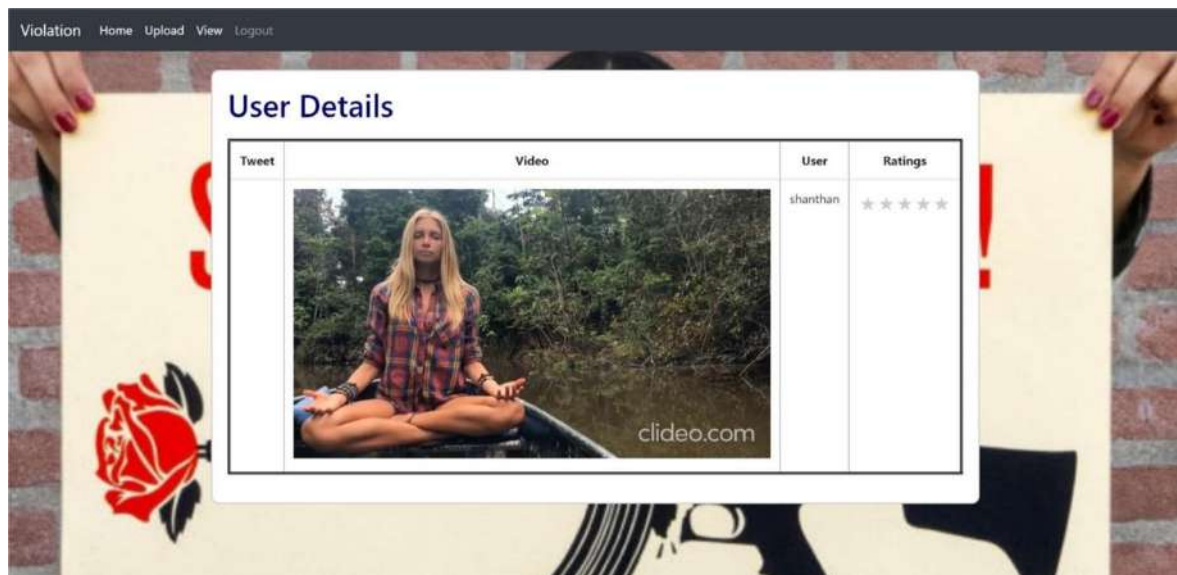
CONCLUSION

In conclusion, this paper has presented a comprehensive framework aimed at enhancing the trustworthiness and security of social multimedia networks (SMNs), particularly in the context of video content delivery. The proliferation of web applications and SMNs has revolutionized global communication, enabling seamless interaction and content sharing among users worldwide. However, this unprecedented connectivity also brings forth challenges related to data management, security, and trust. To address these challenges, we

proposed a generic framework that leverages both human and machine intelligence to ensure the secure delivery of trusted video content over SMNs. Central to this framework is the notion of trust, which is cultivated through the analysis of user history, collaboration, and behavior. By assigning trust levels to users and implementing reputation systems, we aim to establish a network environment characterized by certainty, authenticity, and security in data exchanges. Key components of the proposed framework include modules for trust calculation, voting, incentives, secure video delivery, and video integrity checking. These modules work in concert to enable informed decision-making, content moderation, and quality control, thereby mitigating the spread of unsecured and malicious content within SMNs. Additionally, adaptations to the video player and a video uploading decision process module further enhance content security and integrity. By reducing resource consumption and optimizing content analysis processes, the framework not only enhances network security but also contributes to a more efficient and cost-effective infrastructure for content delivery. Through these efforts, we strive to create a trustworthy SMN ecosystem that prioritizes user safety, content authenticity, and data security.

the proposed framework represents a significant step towards realizing the vision of trustworthy SMNs, where users can confidently engage in content sharing and interaction without compromising their security or integrity. Moving forward, further research and development efforts will be necessary to refine and implement the framework in real-world SMN environments, ultimately fostering a safer and more reliable digital landscape for all users.

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.