



## A SECURE AUTHENTICATED KEY MANAGEMENT PROTOCOL FOR CLOUD COMPUTING ENVIRONMENTS- DESIGN

M.GnanaVardhan<sup>1</sup>, P.Hari Chandana<sup>2</sup>, P.Meghana<sup>3</sup>, N.V.Rajashree<sup>4</sup>, Sd.Ashraf<sup>5</sup>  
<sup>1</sup>Associate Professor, <sup>2,3,4,5</sup> Scholar, Krishna Chaitanya Institute of Technology & Sciences,  
Markapur, A.P, India

---

---

### ABSTRACT:

Due to the dependability and performance of cloud computing technologies developing, many services have migrated to the cloud platform. Due to its ability to simplify service access and protect communication privacy on public networks, three-factor Mutual Authentication and Key Agreement (MAKA) protocols for multi-server architectures are attracting a lot of attention. But a lot of the three-factor MAKA protocols that are now in use either lack a formal security proof, making them open to multiple attacks, or have high computation and transmission costs. Furthermore, most three-factor MAKA protocols don't have a dynamic revocation mechanism, making it challenging for dishonest users to have their access rapidly removed. To address these issues, we provide a tried-and-true dynamic, adjustable, three-factor MAKA protocol. This protocol provides a simple random oracle verification and manages users dynamically using Schnorr signatures. According to a security assessment, our protocol can handle a variety of needs when there are several servers involved. Performance analysis demonstrates that the recommended approach is perfect for smart devices with constrained computing power. The effectiveness of the protocol is seen throughout the whole simulation run.

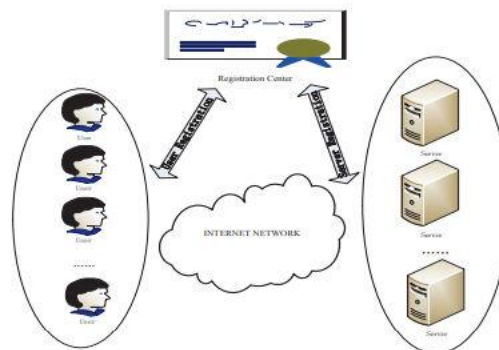
**Keywords:** MAKA, Schnorr, Multi-server

---

---

## 1. INTRODUCTION

In the past 10 years, cloud computing technology has experienced a complete commercialization. It can save costs while enhancing the efficiency of services. A growing number of enterprises are using the cloud platform as a tool for creation, administration, and maintenance. This enables uniform security and operation management for all services on the third-party cloud platform, as indicated in Fig. 1, which not only lessens the cost of local maintenance for these firms. Despite the fact that third-party cloud platforms have more sophisticated technology and more standardised technical standards to ensure that the servers function in a relatively safe environment, users and servers connect over a public network. Therefore, for safe communication, key agreement and verification are essential. By employing mutual authentication and key agreement (MAKA) protocols, attackers are prevented from abusing server resources and from pretending to be the server in order to steal user data. Therefore, the MAKA protocols have undergone much development since Lamport proposed a password-based authentication system. For previous MAKA protocols, a single-server design is envisioned. As the number of Web users grows quickly, the number of cloud servers offering diverse services has significantly expanded. In a single-server arrangement, it is difficult for users to remember a variety of passwords for each server. For multi-server configurations, several academics recommend more flexible MAKA protocols to improve user experience. When paired with the unified management features of the cloud platform, such protocols may be employed with ease. To accomplish mutual authentication and key agreement, users and cloud servers only need to register at the registration centre (RC) for the protocols for multi-server architectures system indicated in fig..



In multi-server situations, the MAKA protocols may be further divided into two categories: two-factor MAKA protocols (identification and password), and three-factor MAKA protocols (identity, password, and biometrics). The study in has shown that a range of techniques, including the guessing password attack, may be used against the password-based MAKA protocols. The cost of a password cracking assault on a password-based system gradually decreases as computers fast advance. On the other side, most users merely use the default password if their smart gadgets don't need them to update it, and most individuals use simple letters or numbers as their passwords. To solve this problem, a variety of biometrics-based MAKA protocols have been proposed. Because biometric identifying keys (palm prints, iris, finger prints, etc.) are distinctive, accessible, and non-transferable, the three-factor MAKA protocols for multi-server situations provide more security than the two-factor protocols. Due to the ease of access to wireless networks, any signals may be intercepted, changed, deleted, and rebroadcast by an adversary. The MAKA protocols must have both anonymity and untrace ability in order to defend against the

aforementioned threats. The three-factor MAKKA protocols that are now in use have the following shortcomings, though.

## 2. LITERATURE SURVEY

A user password authentication method's description makes it obvious that it is secure even if a hacker has access to the system's data and is able to obstruct or eavesdrop on user and system communications. The method assumes the use of a secure one-way encryption technology and may be implemented using a microcomputer at the user's terminal [1].

The advancement of wireless communication systems, embedded systems, and integrated circuit technologies has led to the development of the wireless body area network (WBAN) into a possible networking paradigm. Over the past ten years, WBANs have grown in importance as a component of modern medical systems due to their capability to collect real-time biomedical data via intelligent medical sensors on or near the patient's body and transmit the collected data to remote medical professionals for clinical diagnostics. WBANs not only provide us advantages, but they also make it more difficult to protect patient privacy and data security. In recent years, many anonymous authentication (AA) methods for WBANs have been proposed to boost security by shielding patient identities and medical data. However, many of these remedies are insufficient secure. The most recent AA approach for WBANs is first examined, and its insecurity for usage in medical applications is shown through the deployment of an impersonation attack. We then present a novel AA approach for WBANs and show that it is probably safe. Our extensive study demonstrates that our recommended AA system not only corrects the security issues with prior schemes, but also has comparable client-side computation costs [2].

It is now possible to access a system located far away—possibly in a city or country other than the user's own—and acquire information remotely thanks to the advent of computer networks. The main issue is how well the system can recognise the user in such a situation. This calls for putting in place a method to check the legitimacy of a remote user. In this study, we provide a method for verifying a user's remote login request that is based on 3-D geometric principles. With this approach, we provide two-way mutual authentication, where the user and server independently confirm that they are both legitimate users. The initial phase of this strategy is making the required adjustments to establish a working relationship with the central authority. A user can then register with the server or system after that. The technology enables a user to log in and access the required information after he or she has registered. A legitimate user of our system is always free to modify his password. This technology withstands several attacks without taxing the computer severely [3].

Using a remote user authentication and key agreement system, smart cards are a very practical approach to determine a remote user's eligibility and then enable secure communication. Additionally, due to the fast development of networks and information technology, the bulk of services are provided in multi-server configurations. In this work, we propose a novel smart card-based user authentication and key agreement system for multi-server environments, which offers a considerable increase in functionality at a reduced computational cost. The principal benefits consist of: Users may choose their own passwords, the approach does not require a verification table, users only need to register once at the registration place, the computation costs are minimal, and the transmission costs are minimal. It allows for mutual authentication between users and servers, generates a session key that is acceptable by both sides, and is a nonce-bayed system without a substantial time-synchronization problem [4].

There is a significant weakness in conventional single-server authentication techniques. To utilise a number of network services, a remote user must register their identity and password with these servers. For customers, registering several servers takes a lot of time. Several multi-server authentication methods have recently been developed to overcome this issue. However,

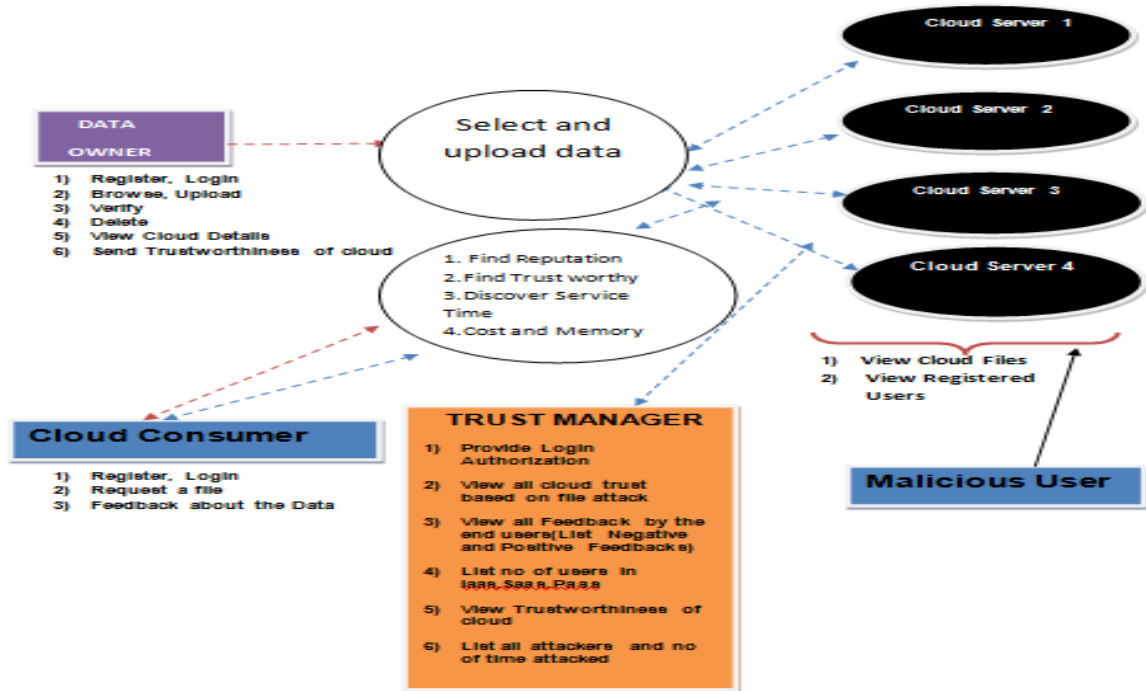
certain systems are either poorly designed or susceptible to specific cryptographic attacks due to high processing costs. Furthermore, these systems do not provide the reliable key agreement mechanism that can provide complete forward secrecy. In light of these factors, this study proposes a new efficient and reliable biometrics-based multi-server authentication with key agreement strategy for smart cards on elliptic curves. The adoption of an encryption scheme (ECC) without a verification table helped to simplify hash operations for all users and take into account multi-server communication scenarios. The recommended method, which makes use of biometrics, can offer a stronger user authentication function. By utilising the ECC methodology, the proposed method may offer a robust key agreement mechanism with the property of total forward secrecy, which also helps to reduce the load on the computing capabilities of smart cards. As a result, the recommended method outperforms comparable multi-server authentication techniques in terms of computing efficiency and strong security. The suggested scheme is especially well suited for use in environments with limited computational and communication resources to access virtual information systems, as it provides security, dependability, and efficiency. These environments include decentralised multi-server network environments like the Internet.

Due to the growing popularity of e-commerce, there are frequently several service servers that provide Internet applications to users, making safe authentication techniques for multi-server setups necessary. On the other hand, in a world where computers is pervasive, customers may access their services via mobile devices. Given the limited energy and computing power of mobile devices, developing a secure authentication system suitable for them is a challenging challenge. In 2008, Tseng et al. introduced a pairing-based user authentication method for mobile clients with limited processing capability. They claimed that their system can be advantageous to the remote user authentication technique for multi-server setups. Some authors are discussed in Secure Authenticated Key Management Protocol in Cloud Computing area [7-35]. Tseng et al.'s, however, are unable to provide mutual authentication and session key agreement.

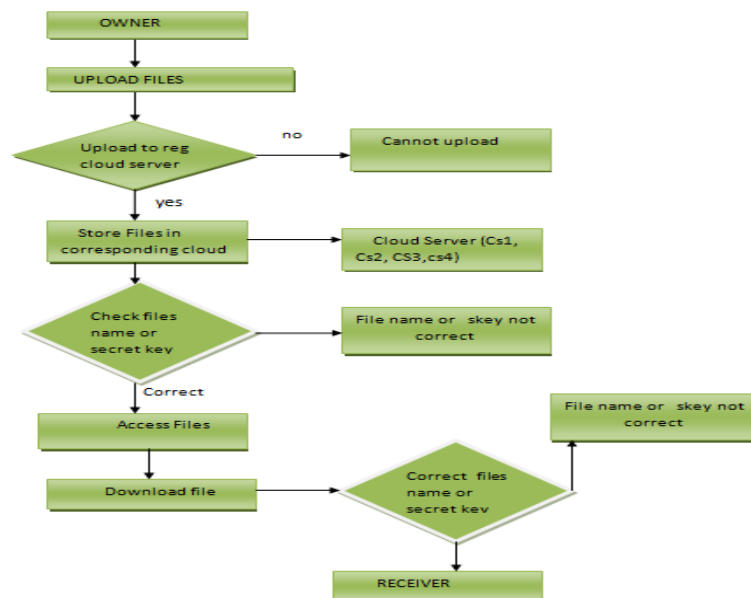
In this work, we will show that the Tseng et al. technique is impervious to insider attacks, offline dictionary assaults, and malicious server attacks. Therefore, we offer a special pairing-based remote user authentication solution for multi-server scenarios. The recommended method, which is based on self-certified public keys, initially provides a more secure key distribution among the service servers (SCPks). Mutual authentication and session key agreement are possible with the described method. The recommended technique reinforces the password changing phase with the help of the registration server to protect against an offline dictionary attack caused by a security flaw on mobile devices.

### **3. SYSTEM DESIGN**

#### **3.1 System Architecture**



### 3.2 FLOWCHART:



## 4. Implementation

### 4.1 Modules Description:

**i) Data Owner:** The cloud server (CS1,CS2,CS3,CS4) must first receive the data owner's registration information in this module. To access the appropriate cloud server where he registered, the data owner will log in. The file will be uploaded to the cloud server by the data owner (CS1, CS2, CS3, CS4) The data owner verifies the security of the file he uploaded. The data owner can view the total number of files uploaded to the appropriate cloud servers (CS1,CS2,CS3,CS4) The trust manager will receive the file from the data owner and store it on the relevant cloud servers (CS1,CS2,CS3,CS4)

**ii) Cloud Server:** To provide services for data storage, a cloud is run by a cloud server. Data owners encrypt and store their files in the cloud for sharing with other cloud users. In order to access shared data files, data consumers must download and decode the encrypted data files they need from the cloud.

**iii) Trust Manager:** With the aid of the trust manager, both the data owner and the end user may log in. The trust manager has access to the cloud status. End-user feedback, which includes both positive and negative remarks, is available to trust managers. A list of cloud service users is provided by Trust Manager (IAAS, PAAS, SAAS). The trust management can see who has attacked which cloud servers (CS1,CS2, CS3,CS4) and how long the assaults have lasted.

**iv) Cloud Consumer:** Users of the cloud must first sign up with the particular cloud server they plan to utilise (CS1, CS2, CS3, CS4). To access the cloud where he registered, the user needs login in. consumer comment on the cloud data (positive or negative feedback)

**v) Attacker:** Attacker will examine cloud files and registered users.

- a) **Collusion Attacks – to make false comments** regarding the cloud
- b) **Sybil Attacks -** When user uses more transaction per day (Exceeds the limit which is assigned by the Trust Manager)

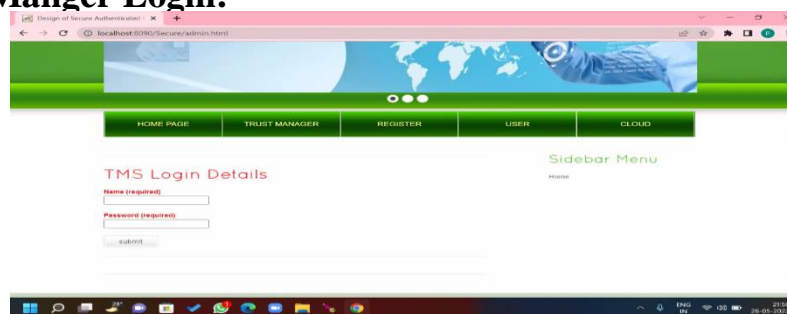
## 4.2 Screenshots

### Home Page:



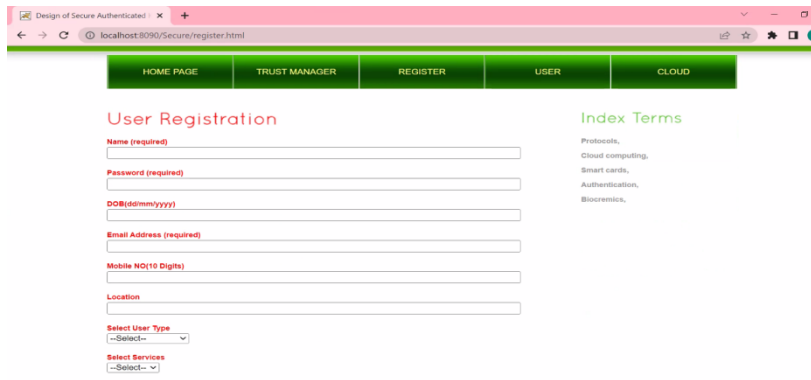
The Home Page is the Main Page that Contains The TrustManager ,Register,User,Cloud Tabs

### Trust Manger Login:



Trust Manger Login Page need the Login Details of The Owner Name And Valid Password

## Registration Form:

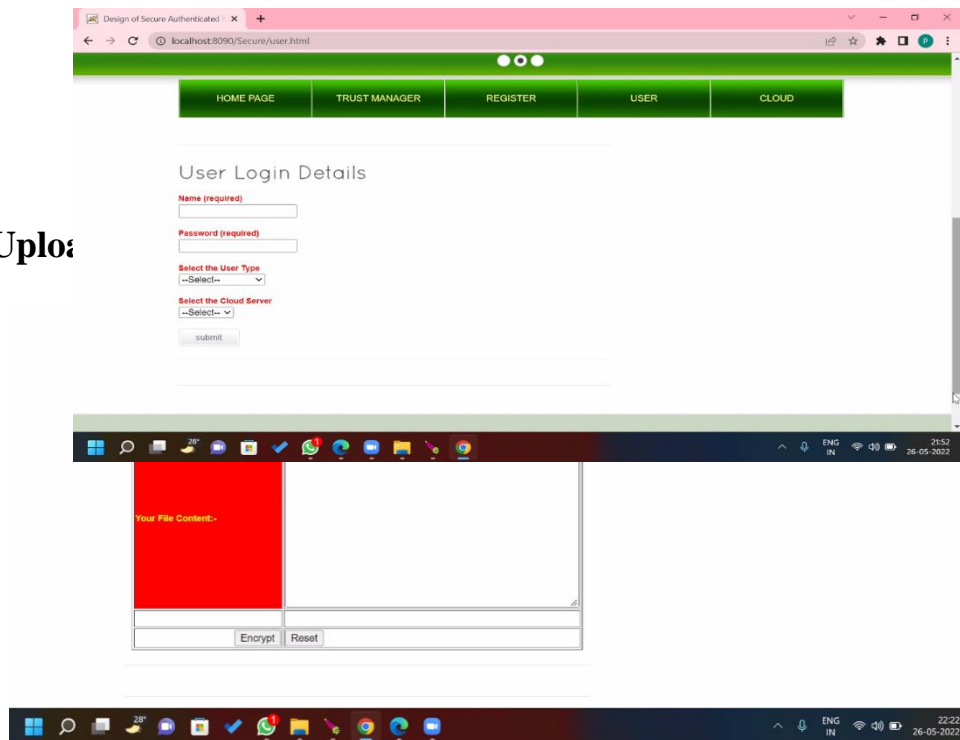


The screenshot shows a web browser window with the URL `localhost:8090/Secure/register.html`. The page has a green navigation bar with buttons for HOME PAGE, TRUST MANAGER, REGISTER, USER, and CLOUD. The main content area is titled "User Registration" and contains several input fields: Name (required), Password (required), DOB (dd/mm/yyyy), Email Address (required), Mobile NO (10 Digits), Location, Select User Type (dropdown menu), and Select Services (dropdown menu). To the right of the registration form is a section titled "Index Terms" with a list of terms: Protocols, Cloud computing, Smart cards, Authentication, and Biometrics.

For Login the User Should Register the Details in the Registration Form

## User Login:

Upload



The screenshot shows a web browser window with the URL `localhost:8090/Secure/user.html`. The page has a green navigation bar with buttons for HOME PAGE, TRUST MANAGER, REGISTER, USER, and CLOUD. The main content area is titled "User Login Details" and contains several input fields: Name (required), Password (required), Select the User Type (dropdown menu), and Select the Cloud Server (dropdown menu). Below the input fields is a "submit" button. The browser window also shows a taskbar at the bottom with various application icons and system tray icons.

The User Login to Verify the files or to access the files

## Cloud:

The User can Upload Files from UPLOADFILE Tab for Secure Files



## 5. Conclusion

To defend two-factor MAKAs from the depletion of password attack, many three-factor MAKAs techniques have been proposed. All three-factor MAKAs protocols, however, are essentially devoid of a dynamic user management system and rigorous proofs. In order to give more dynamic user management and higher security, this research introduces a unique three-factor MAKAs protocol that supports dynamic revocation and provides formal proof. Our protocol meets the requirements for multi-server environments in terms of security, as shown by the security. On the other hand, because of the careful examination of performance, our method keeps efficiency while improving function. On the other hand, the recommended strategy provides important advantages in terms of overall computation time. Future work will be implemented using a real cloud situation. In order to safeguard additional security features in cloud computing, we offer secure authentication utilising biometric or retina scanning technology.

## References

- [1] L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, vol. 24, no. 11, pp. 770–772, 1981
- [2] D. He, S. Zeadally, N. Kumar, and J. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Syst. J.*, vol. 22, pp. 1–12, 2016.
- [3] L. Li, L. Lin, and M. Hwang, "A remote password authentication scheme for multi server architecture using neural networks," *IEEE Trans. Neural Networks.*, vol. 12, no. 6, pp. 1498–1504, Nov.2001.
- [4] W. Juang, "Efficient multi-server password authenticated key agreement using smart cards," *IEEE Trans. Consumer Electron.*, vol. 50, no. 1, pp. 251–255, Feb.2004.
- [5] C. C. Chang and J. S. Lee, "An efficient and secure multi-server password authentication scheme using smart cards," in *Proc. Int. Conf. Cyberworlds*, 2004, pp. 417–422
- [6] Y. Liao and C. Hsiao, "A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients", *Future Generation Comput. Syst.*, vol. 29, no. 3, pp. 886-900, 2013.
- [7] J. Ronson, *So You've Been Publicly Shamed*. Picador, 2015.
- [8] E. Spertus, "Smokey: Automatic recognition of hostile messages," in *AAAI/IAAI*, 1997, pp. 1058–1065.
- [9] S. Sood, J. Antin, and E. Churchill, "Profanity use in online communities," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2012, pp. 1481–1490.
- [10] S. Rojas-Galeano, "On obstructing obscenity obfuscation," *ACM Transactions on the Web (TWEB)*, vol. 11, no. 2, p. 12, 2017.
- [11] E. Wulczyn, N. Thain, and L. Dixon, "Ex machina: Personal attacks seen at scale," in *Proceedings of the 26th International Conference on World Wide Web*. International World Wide Web Conferences Steering Committee, 2017, pp. 1391–1399.
- [12] A. Schmidt and M. Wiegand, "A survey on hate speech detection using natural language processing," in *Proceedings of the Fifth International Workshop on Natural Language Processing for Social Media*. Association for Computational Linguistics, Valencia, Spain, 2017, pp. 1–10.



- [13] Hate-Speech, “Oxford dictionaries,” retrieved August 30, 2017 from [https://en.oxforddictionaries.com/definition/hate speech](https://en.oxforddictionaries.com/definition/hate%20speech).
- [14] W. Warner and J. Hirschberg, “Detecting hate speech on the world wide web,” in Proceedings of the Second Workshop on Language in Social Media. Association for Computational Linguistics, 2012, pp. 19–26.
- [15] I. Kwok and Y. Wang, “Locate the hate: Detecting tweets against blacks.” in AAAI, 2013.
- [16] P. Burnap and M. L. Williams, “Cyber hate speech on twitter: An application of machine classification and statistical modeling for policy and decision making,” Policy & Internet, vol. 7, no. 2, pp. 223–242, 2015.
- [17] Lee-Rigby, “Lee rigby murder: Map and timeline,” retrieved December 07, 2017 from <https://http://www.bbc.com/news/uk-25298580>.
- [19] Z. Waseem and D. Hovy, “Hateful symbols or hateful people Predictive features for hate speech detection on twitter.” in SRW@ HLT-NAACL, 2016, pp. 88–93.
- [20] P. Badjatiya, S. Gupta, M. Gupta, and V. Varma, “Deep learning for hatespeech detection in tweets,” in Proceedings of the 26th International Conference on World Wide Web Companion. International World Wide Web Conferences Steering Committee, 2017, pp. 759–760.
- [21] D. Olweus, S. Limber, and S. Mihalic, “Blueprints for violence prevention, book nine: Bullying prevention program,” Boulder, CO: Center for the Study and Prevention of Violence, 1999.
- [22] P. K. Smith, H. Cowie, R. F. Olafsson, and A. P. Liefoghe, “Definitions of bullying: A comparison of terms used, and age and gender differences, in a fourteen-country international comparison,” Child development, vol. 73, no. 4, pp. 1119–1133, 2002.
- [23] R. S. Griffin and A. M. Gross, “Childhood bullying: Current empirical findings and future directions for research,” Aggression and violent behavior, vol. 9, no. 4, pp. 379–400, 2004.
- [24] H. Vandebosch and K. Van Cleemput, “Defining cyberbullying: A qualitative research into the perceptions of youngsters,” CyberPsychology & Behavior, vol. 11, no. 4, pp. 499–503, 2008.
- [25] H. Vandebosch and K. Van Cleemput, “Cyberbullying among youngsters: Profiles of bullies and victims,” New media & society, vol. 11, no. 8, pp. 1349–1371, 2009.
- [26] K. Dinakar, B. Jones, C. Havasi, H. Lieberman, and R. Picard, “Common sense reasoning for detection, prevention, and mitigation of cyberbullying,” ACM Transactions on Interactive Intelligent Systems (TiiS), vol. 2, no. 3, p. 18, 2012.
- [27] P. Singh, T. Lin, E. T. Mueller, G. Lim, T. Perkins, and W. L. Zhu, “Open mind common sense: Knowledge acquisition from the general public,” in OTM Confederated International Conferences “On the Move to Meaningful Internet Systems”. Springer, 2002, pp. 1223–1237.
- [28] H. Hosseinmardi, S. A. Mattson, R. I. Rafiq, R. Han, Q. Lv, and S. Mishra, “Detection of cyberbullying incidents on the instagram social network,” arXiv preprint arXiv:1503.03909, 2015.
- [29] J. Cheng, C. Danescu-Niculescu-Mizil, and J. Leskovec, “Anti social behavior in online discussion communities.” in ICWSM, 2015, pp. 61–70.
- [30] J. Cheng, C. Danescu-Niculescu-Mizil, J. Leskovec, and M. Bernstein, “Anyone can become a troll,” American Scientist, vol. 105, no. 3, p. 152, 2017.
- [31] P. Tsantarliotis, E. Pitoura, and P. Tsaparas, “Defining and predicting troll vulnerability in online social media,” Social Network Analysis and Mining, vol. 7, no. 1, p. 26, 2017.
- [32] S. O. Sood, E. F. Churchill, and J. Antin, “Automatic identification of personal insults on social news sites,” Journal of the Association for Information Science and Technology, vol. 63, no. 2, pp. 270–285, 2012.
- [33] SK Althaf Hussain Basha, B Sasidhar, “A Review on the Challenges of E-Commerce Security Issues, Privacy, Trust and Solutions”, International Conference on Consumer Dynamic and Marketing Strategies in Globalized Economic Era-Perspectives and Challenges, GRIET, Hyderabad, 2013.
- [34] SK Althaf Hussain Basha, B Sasidhar, “ The Effect of E-Commerce Applications on Marketers and Consumers: A Case Study ”, International Conference on Consumer Dynamic and Marketing Strategies in Globalized Economic Era-Perspectives and Challenges, GRIET, Hyderabad, 2013.
- [35] SK. Althaf Husain Basha, SkNikhath, P YejdaniKhan . “Safety Fear/Attacks Current in Cloud Environment”, Volume 4, Issue 2, November 2019, pp. 324-330, International Journal of Recent Issues on Computer Science & Electronics (IJRICSE)