ISSN (E): 2959-3921
(P): 2959-393X (Provisional)
DOI: https://doi.org/10.59122/134CFC9



Ethiopian International Journal of Engineering and Technology (EIJET)
Volume 1, Issue 1, 2023

Designing a Framework for Cyber Protection based on Unique Identification to Improve the Security of Ethiopian Social Media Users over Facebook

Basha Kesim[1*]

[1] Faculty of Computing and Software Engineering, Arba Minch University, Ethiopia

*Corresponding Author's Email: bashirkasim59@gmail.com

Abstract

Social media platforms such as Facebook, which has over 2.6 billion monthly active users, play a major role in global communication. However, Facebook users often face various security threats, including impersonation and the spread of false information. In Ethiopia, these issues have become increasingly prevalent. Therefore, it is essential to develop effective countermeasures to address and mitigate such challenges. This research aims to develop a Unique-ID-based Cyber Defense Framework designed to strengthen the security of Facebook users and prevent the creation of fake profiles and impersonation by malicious actors. This study employed an exploratory and constructive research design, utilizing surveys and in-depth interviews, to develop a Unique-ID-based Cyber Defense Framework. The proposed framework leverages Addis Ababa's Digital Residential ID to authenticate users by cross-referencing their information with a resident database. A prototype was developed and tested, with 87% of respondents accepting the solution as a positive contribution to cybersecurity. The system is designed to verify user uniqueness during Facebook account creation, thereby preventing the establishment of fake or duplicate accounts.

Keywords: Country Code, Cyber Defense, Facebook, Fake Profile, Impersonation, Unique Id, Security Threat

I. Introduction

Accessing information anywhere, any time, and in any condition without the restriction of location was one of the features of the 21st century. Social media is now among the most influential media for the transmission, dissemination, and exchange of information and knowledge. It is used by billions of users to network with other users [1] [2]. Social networking platforms, including Facebook, LinkedIn, and Twitter, have emerged as predominant global communication channels, experiencing exponential user growth. There are more than 3.81 billion active users of social media networks today. Of all social media, Facebook is the largest with 2.6 billion monthly active users. Users of the maximum social media network have more than 200 friends [3] [4]. In addition to its benefits, social media has several drawbacks including security

Received: *19 March 2022;* ***Revised:*** *27 March 2023;* ***Accepted:*** *2 May 2023.* ***Published:*** *30 April 2023.*
Corresponding author- ***Basha Kesim***

risks. The key problem with social media is the presence of fake accounts and online impersonations [5], especially on Facebook. As there is a lack of effective identity-proving mechanisms, anyone can set up a fake profile in the name of someone else to post negative and offensive content through the account [6]. Fake accounts are created to access people's information and post fabricated content since not all Facebook users check and verify the accounts before accepting the request from them [2] [7] [8].

Social network operators use several authentication methods to ensure that the individual registered on the social network is a natural person. Methods such as CAPTCHA, recognition of friends' images, and multi-factor authentication are used [5] [19] [11]. On Facebook, with multiple profiles, a single user can represent his identity because there is a lack of an effective identity verification process [12]. Facebook currently serves mainly as a channel for hate speech, intolerance, and increased discrimination against a specific ethnicity, religion, or gender [11]. In Ethiopia, Facebook's spread of hate speech and disinformation has grown exponentially in a couple of years. In January 2020, there were 6.20 million social media users in Ethiopia, as described by the study of world internet statistics 2020. Facebook is, therefore, the most prevalent use, and more than six million people use Facebook in Ethiopia [13].

There is a lack of methods for checking the source, which means it is difficult to trace the identity of the account owner [14]. Currently, there is a lack of effective Facebook user virtual identity verification frameworks. By using this chance bad users create fake accounts and impersonate someone to disseminate fabricated information that is targeted and discriminates against individuals or groups based on their ethnicity, religion, and gender. Ethiopia has also suffered from Facebook because it acts primarily as a channel for hate speech, intolerance, and increased prejudice against a specific race, religion, and gender. Thus, these issues are causing tension between governments and individuals. In 2016 the Ethiopian government blocked Facebook many times because it was causing extensive instability in the country. Because misinformation can spread quickly via Facebook, the government confirmed to block social media totally from the country to stop the spread of hate and ethnic cleansing propaganda messages. Therefore, this shows Ethiopia's internet control operates mainly outside of a formal regulatory framework by blocking the internet totally from the country. And this is not effective, efficient, or productive. For example, Brookings Institution's report shows that Ethiopia, between mid-2015 and mid-2016, lost t $9 million US dollars due to internet shutdowns.

Therefore, this researcher motivates the researchers to build a system that can improve the verification of user identity on Facebook by developing an improved framework for enforcing the users to create their accounts with their genuine information. The implementation of the unique identification of user identity on Facebook for account creation and login is addressed in this research paper.

Received: *19 March 2022;* ***Revised:*** *27 March 2023;* ***Accepted:*** *2 May 2023.* ***Published:*** *30 April 2023.*
Corresponding author- ***Basha Kesim***

II. Literature Review

Table I: Review of Related Works with Critical Remarks

No	Authors	Significant Contributions	Critical Remarks
1	Michail Tsikerdekis and Sherali Zeadally [18]	The researchers tried to discuss how to decrease identity deception by securing social media design and applying psychological pressure to deceivers. To prevent deceivers, they recommended different techniques like biometric authentication is one of them.	This paper tried to discuss how to decrease identity deception by securing social media design and applying psychological pressure to deceivers. To prevent deceivers, they recommended different techniques like biometric authentication is one of them. The study was very relevant to our paper. However, it failed to explain how to verify the authenticity of the user identity, especially for Facebook, to prevent fake or forgery account creation and they missed explaining how to evade social media problems
2	Nadir AI Naqbi, Nail Al Momani, and Amanda Davies [19]	This paper explored the influence of social media as a threat to national security-related issues like social, Economic, and political disorders. This paper suggested the community awareness	This paper is relevant to our study. This research explored Arab Emirates data to discuss how to decrease identity deception by securing social media design and applying psychological pressure to deceivers. To prevent deceivers, they recommended biometric authentication.
4	Amitvikram Nawalagatti [20]	This study discusses the adverse impact of social media on users' privacy and security. In this paper, researchers tried to explain that social media are not suitably monitored and accounts are not properly verified. The study revealed many threats created by social media and proposed solutions	This study was very focused and found interesting to our research. The solution proposed by this research is very shallow and does not provide any concrete solution to secure the users' privacy like creating a strong password by complex combinations of alphabets, characters and special characters along with strong authorization on network access etc.

Received: *19 March 2022;* ***Revised:*** *27 March 2023;* ***Accepted:*** *2 May 2023.* ***Published:*** *30 April 2023.*
Corresponding author- ***Basha Kesim***

ISSN (E): 2959-3921
(P): 2959-393X (Provisional)
DOI: https://doi.org/10.59122/134CFC9

III. Research Methodology

This study employed a mixed-methods research design, combining exploratory and constructive approaches. Both qualitative and quantitative data were collected to gather comprehensive and relevant evidence. Therefore, a structured questionnaire and In-depth interview were prepared and distributed among selected social media users, and interviews were conducted with INSA.

A. Data Collection Procedures

The summary of data collection methods from both primary and secondary data sources is described in the following Fig. 1.

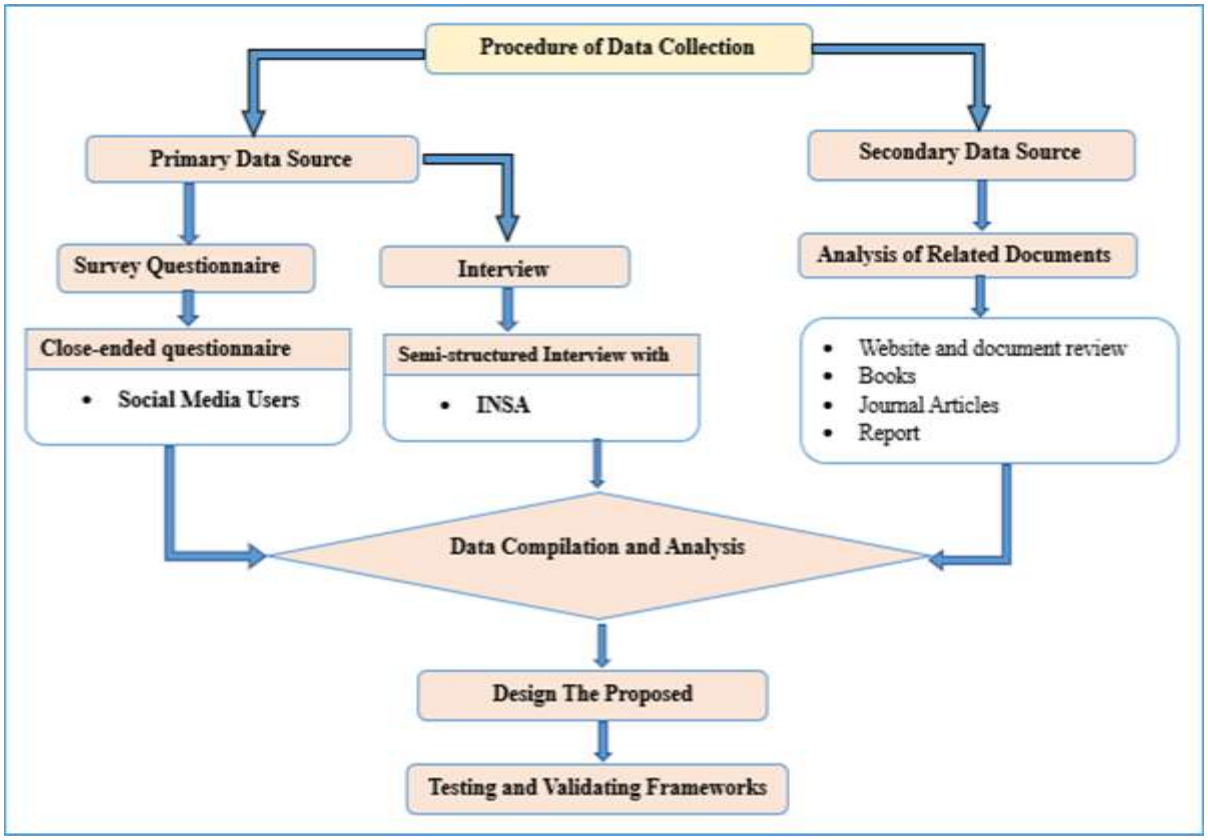


Fig. 1: Summary of data collection methods

B. Sampling Design

This study used the purposive sampling method. The person who does use social media in Ethiopia had the chance to be included in the study. This research study's sample size was 342. Three hundred thirty-eight (338) social media users were chosen for the survey questionnaire and 4 for the interview to collect the primary data.

Received: *19 March 2022;* ***Revised:*** *27 March 2023;* ***Accepted:*** *2 May 2023.* ***Published:*** *30 April 2023.*
Corresponding author- ***Basha Kesim***

ISSN (E): 2959-3921
(P): 2959-393X (Provisional)
DOI: https://doi.org/10.59122/134CFC9

IV. Data Analysis and Discussion

A. Demography of the Respondents

Fig. 2, shows the data of the respondents' demography like gender, age, occupation and education levels.

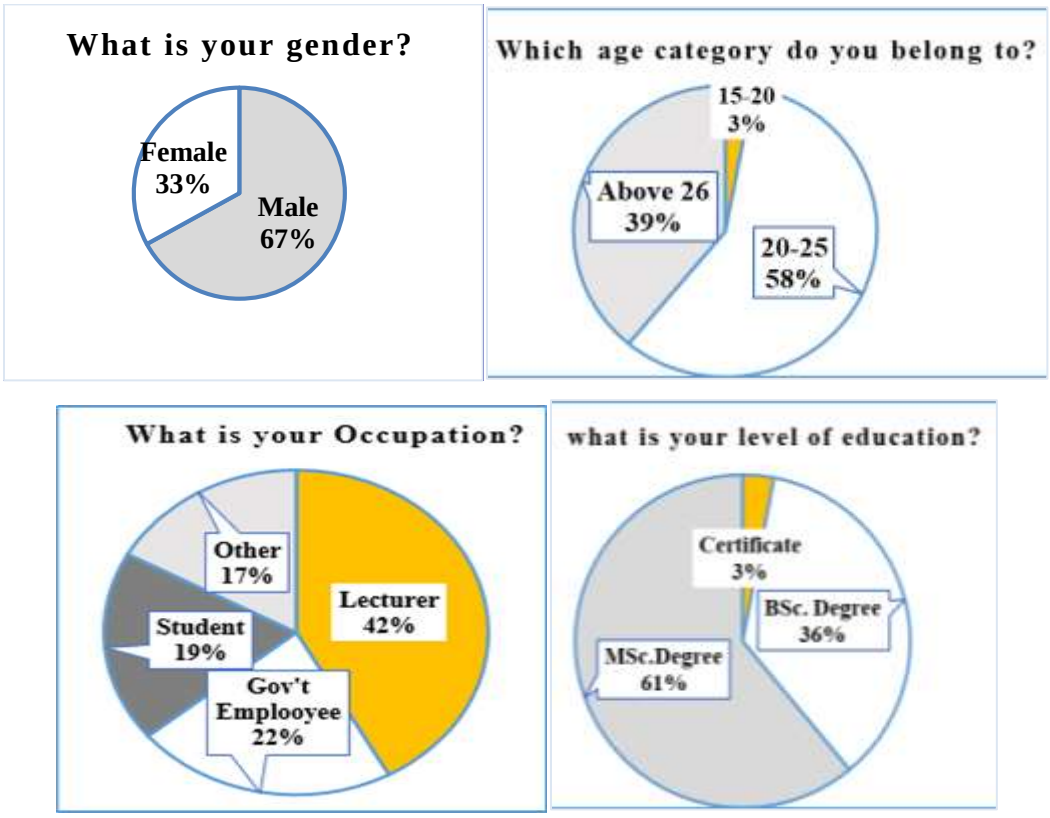


Fig. 2: Respondents' Demography Pie charts

How do you rate your participation in discussions on social media, especially Facebook?

As illustrated in Fig. 3, a majority of users do not participate in discussions on Facebook. This lack of engagement can be attributed to several factors.

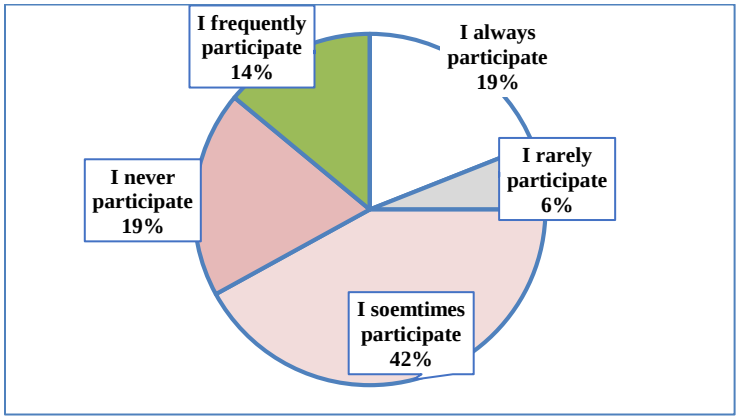


Fig. 3: Participation rate of respondents on Facebook

Received: *19 March 2022;* ***Revised:*** *27 March 2023;* ***Accepted:*** *2 May 2023.* ***Published:*** *30 April 2023.*
Corresponding author- ***Basha Kesim***

ISSN (E): 2959-3921
(P): 2959-393X (Provisional)
DOI: https://doi.org/10.59122/134CFC9

If your participation in discussions is minimal, what prevented you from engaging in discussions on Facebook?

This follow-up question asks respondents to explain their minimal participation on Facebook, as indicated in Fig. 3. Fig. 4 result implies that the reason why respondents' participation is minimal was that Facebook became the Media on which fake information can be propagated.

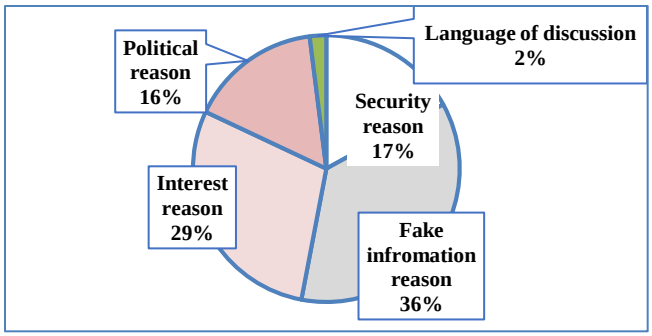


Fig. 4: Reasons that prevent the respondent from participating on Facebook

What kind of information do you give to open a Facebook account?

As Fig. 5 shows the maximum number of respondents are not providing truthful information, and this specifies the existing security checking gap on Facebook. 62% (real/genuine) is greater than 38% (fake) but when we see the effect level of this amount, it is very big.

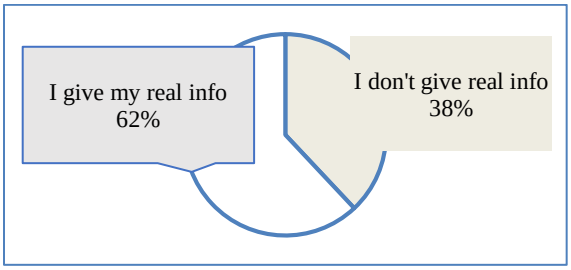


Fig. 5: Rate of access behavior of Facebook by Respondents

Do you trust the information you get on social media especially on Facebook?

The phenomenon on Fig. 6 confirms that the source of information propagated on Facebook was not trusted as verified and authenticated.

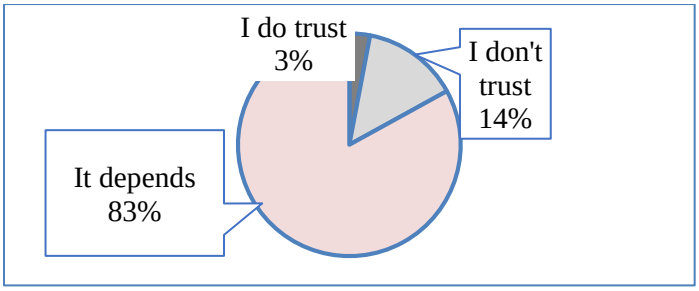


Fig. 6: The rate of trust in the information from Facebook

Received: *19 March 2022;* ***Revised:*** *27 March 2023;* ***Accepted:*** *2 May 2023.* ***Published:*** *30 April 2023.*
Corresponding author- ***Basha Kesim***

ISSN (E): 2959-3921
(P): 2959-393X (Provisional)
DOI: https://doi.org/10.59122/134CFC9

Can you believe that the current Facebook page verifies the real identity of the users?

As demonstrated in Fig. 7, existing Facebook security requires an immediate framework to enhance user protection. The primary recommendation is the implementation of a system that solves identity verification and authentication, thereby preventing identity theft by ensuring a strict match between a user's physical and digital identity.

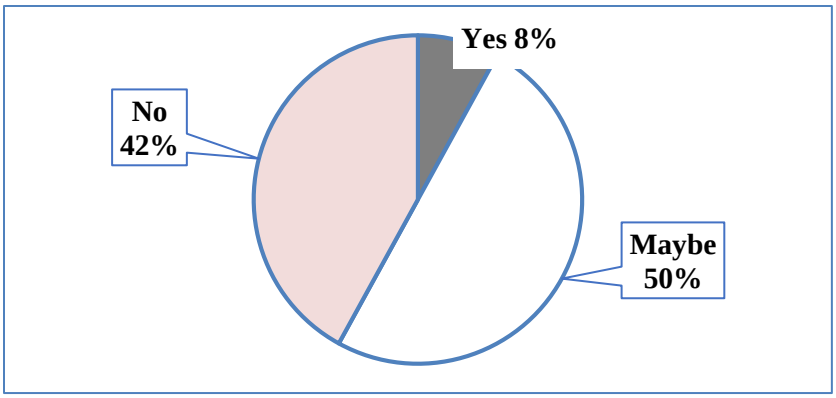


Fig. 7: The rate of identity verification of Facebook

Can you believe that the required information to create an account on Facebook is enough to avoid fake accounts and duplicate account creation?

As Fig. 8 shows, the highest number of respondents responded with "**NO,**" which means the current Facebook page was easy for creating a fake or duplicate account as described in the literature review part.

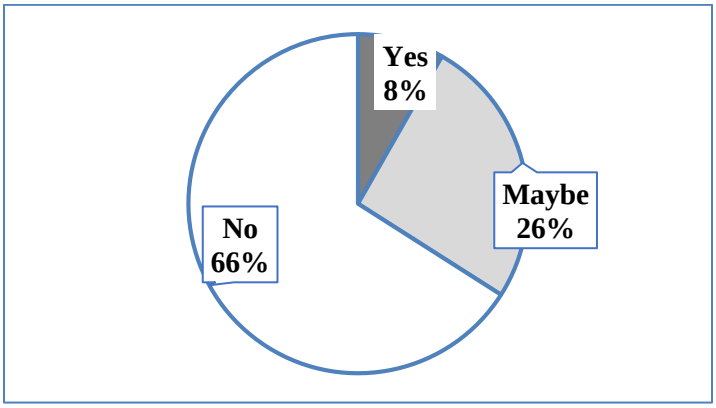


Fig. 8: Rate of respondents on duplicate and fake accounts inhibition way of Facebook

Can Facebook features such as anonymity and ease in having fake accounts, names and identities facilitate the discourse of hate speech as these features help the abusers go undetected and unpunished in our country?

The result on Fig. 9 shows that Facebook can be the instrument of hate speech dissemination and does facilitate and become a safe port for individuals, groups, and activists who intend to post toxic or offensive ideas. 61% of respondents have responded by agreeing.

Received: *19 March 2022;* ***Revised:*** *27 March 2023;* ***Accepted:*** *2 May 2023.* ***Published:*** *30 April 2023.*
Corresponding author- ***Basha Kesim***

ISSN (E): 2959-3921
(P): 2959-393X (Provisional)
DOI: https://doi.org/10.59122/134CFC9

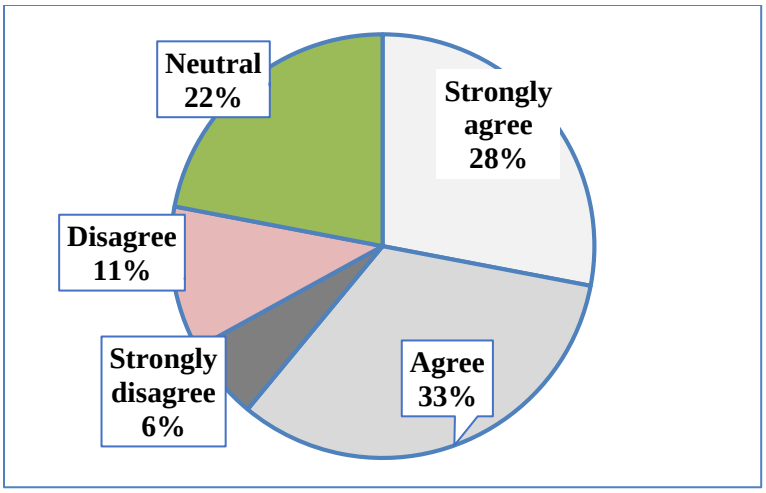


Fig. 9: Rate of respondents on the facilitation of hate speech by Facebook**.**

Currently, in our country, are there political activists with an interest to destabilize the country that are going to abuse Facebook features for getting speedy and vast audience connectivity?

Fig. 10 result specifies that there was a significant and vital need to develop an improved security framework that enhances the existing unique verification mechanism of Facebook accounts to satisfy the user's requirements. This can be done by bringing in a suitable alternative to control and prevent those who use Facebook for illegal activity from abusing Facebook features.

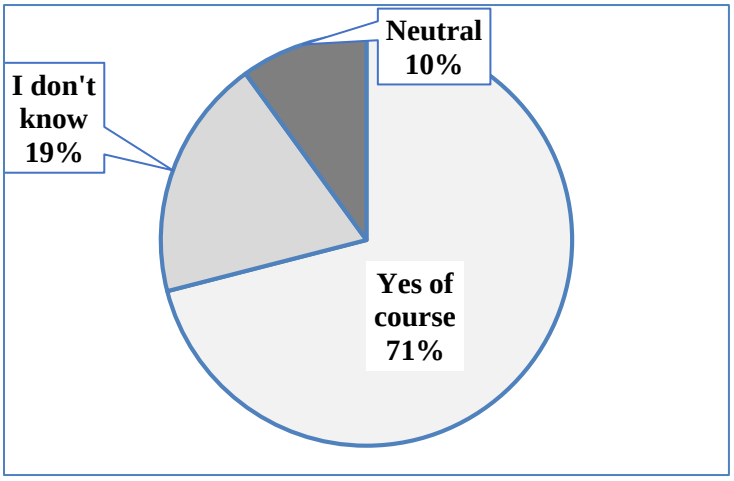


Fig. 10: Rate of respondents on the facilitation of political activists with an interest to destabilize the country by abusing on Facebook**.**

Why did the government block Facebook and other related media in the past few years?

The phenomenon on Fig. 11 indicates a strong need by Facebook users to develop an advanced framework that enhances the security on Facebook to prevent Facebook from becoming the media on which hateful information was propagated and to achieve stability and security for society.

Received: *19 March 2022;* ***Revised:*** *27 March 2023;* ***Accepted:*** *2 May 2023.* ***Published:*** *30 April 2023.*
Corresponding author- ***Basha Kesim***

ISSN (E): 2959-3921
(P): 2959-393X (Provisional)
DOI: https://doi.org/10.59122/134CFC9

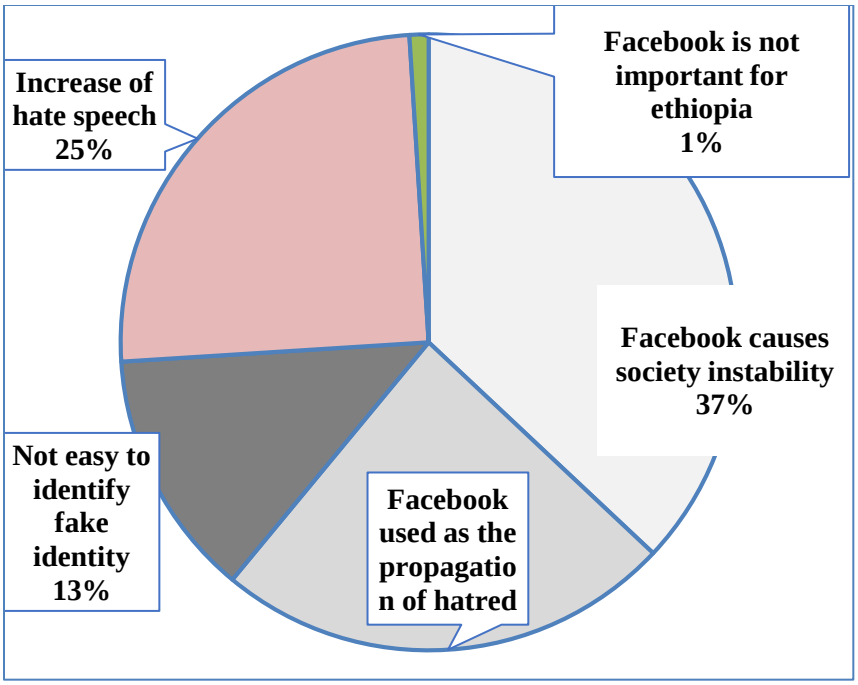


Fig. 11: Rate of respondents on the reason for blocking the Facebook site

How often do you use Facebook?

As per the results on Fig. 12 below, the maximum number of people are using Facebook as media in which they post their everyday thoughts, feelings and activities.

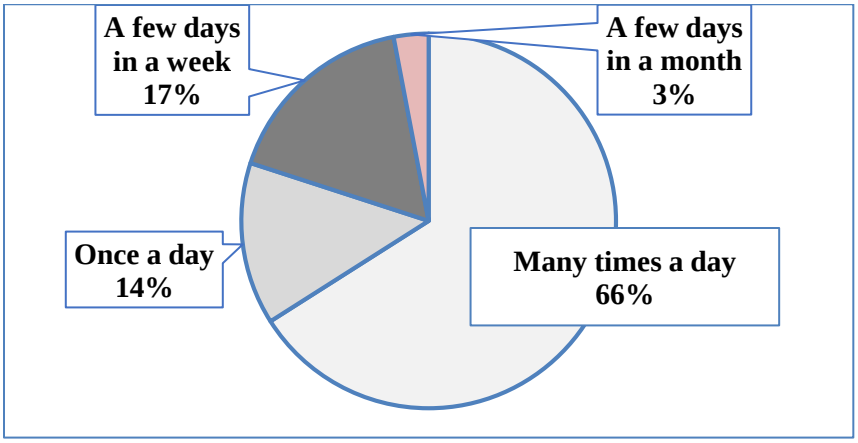


Fig. 12: The rate of how often the respondents use Facebook.

For what purpose are you using Facebook?

The phenomena on Table II indicate that the maximum number of respondents are using Facebook for the excellent purpose that was appreciated. Still, some respondents use Facebook for illegal purposes like posting about political discrimination, posting information on touching others' religion, and negatively criticizing the government using the account created by Fake evidence.

Received: *19 March 2022;* ***Revised:*** *27 March 2023;* ***Accepted:*** *2 May 2023.* ***Published:*** *30 April 2023.*
Corresponding author- ***Basha Kesim***

ISSN (E): 2959-3921
(P): 2959-393X (Provisional)
DOI: https://doi.org/10.59122/134CFC9



Ethiopian International Journal of Engineering and Technology (EIJET)
Volume 1, Issue 1, 2023

Table II: Purpose of Using Facebook By Respondents**.**

Purpose of using Facebook by respondents	Frequency (%)
To read news	32.65%
To know about a friend's life	25.49%
To share political, dissect	19.44%
To criticize the government	3.04%
To present political ideas	6.13%
Discuss the issue of cultural identity	5.10%
Commenting on people who are impacting my religion	8.15%

Do you check the source of the message before liking, reacting to, sharing or commenting on the post when using Facebook?

Fig. 13 indicates that the maximum number of users on Facebook accept the content without checking the truthfulness of the posted information.

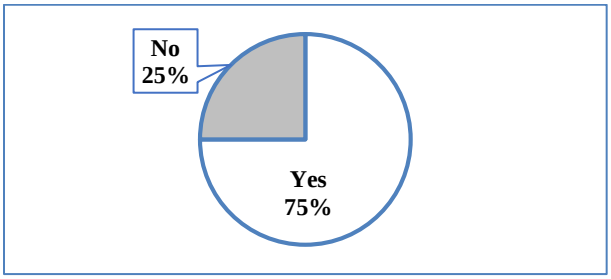


Fig. 13: Rate of respondents that are checking the source of content on Facebook

Do you agree that Facebook plays a substantial role in catalyzing hate speech, discrimination in society, increasing instability, and lack of peace in our county?

The phenomenon on Fig. 14 suggests a strong need for an urgent mechanism to restrict scammers from fake information dissemination on Facebook.

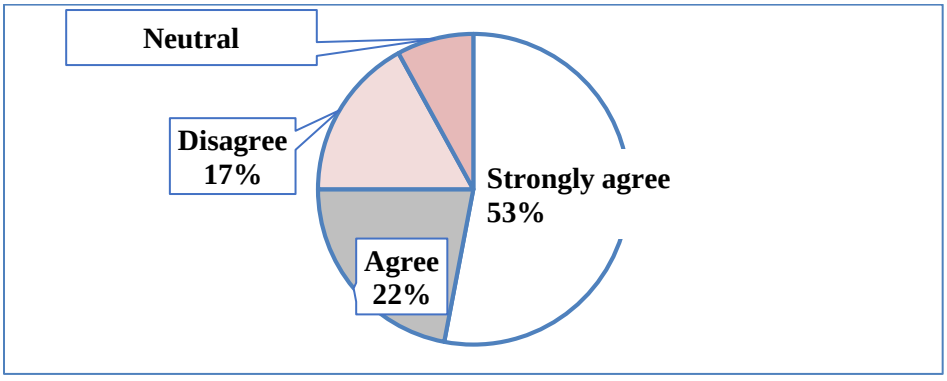


Fig. 14: Rate of Respondents on Facebook used as the publication of the dangerous idea

Received: *19 March 2022;* ***Revised:*** *27 March 2023;* ***Accepted:*** *2 May 2023.* ***Published:*** *30 April 2023.*
Corresponding author- ***Basha Kesim***

ISSN (E): 2959-3921
(P): 2959-393X (Provisional)
DOI: https://doi.org/10.59122/134CFC9



Ethiopian International Journal of Engineering and Technology (EIJET)
Volume 1, Issue 1, 2023

Would you need improved frameworks that enhance the security checking for verifying user identity on Facebook?

The percentage on Fig. 15 indicates that the highest number of respondents or the highest number of Facebook users need an urgent development of a better-quality regulatory and control framework to enhance users' security and to prevent Fake accounts and duplicate account creation.

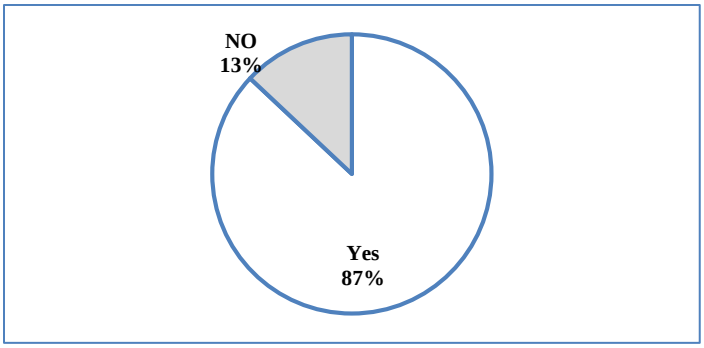


Fig. 15: the need for improved security Frameworks on Facebook

V. Developing a Regulatory and Control Framework

Proposed Solution and its functionalities

This research paper introduces an innovative solution to protect and prevent creating a fake profiles, duplicate or redundant accounts, and impersonation. This research study presents a new concept to identify whether the users are providing factual personal information uniquely or not. The items that can be used to verify the user's identity should be unique.

VI. Results Discussion

Creating a Profile on Facebook

First, the user accesses the Facebook platform through the internet and completes the registration form. In addition to the standard information typically required, two additional attributes are introduced to verify whether the user's input matches the official data stored in the country's digital residential ID card database. After filling out the form, the user submits the information to the Facebook server by clicking the registration button.

Next, the Facebook server performs data validation before allowing the account to be created. Server-side authentication and verification processes are carried out to confirm the accuracy of the user-provided information. The submitted data is cross-checked against the national digital residential ID database to determine whether the individual exists in the system. This verification process uses a unique ID as the primary key and the country code to identify the user's location during account creation.

Received: *19 March 2022;* ***Revised:*** *27 March 2023;* ***Accepted:*** *2 May 2023.* ***Published:*** *30 April 2023.*
Corresponding author- ***Basha Kesim***

This takes place every time a new user tries to create an account on the Facebook server. Generally, as everybody cannot provide an identity card independently, the institutions that have authority are responsible for giving proper unique identifiers.

Login to Profile

The login process was similar to the existing one.

Significant Components of the Proposed Framework

Fig. 16 illustrates the general framework for enhancing Facebook account security through digital ID verification. The architecture is divided into two primary sides—the User Side and the Server Side—each comprising specific components with distinct functions, as detailed below.

User Side Components:

- **User:** An individual attempting to access or use the Facebook platform.
- **Internet:** The global network facilitating communication between the user and online services.
- **Facebook Website:** The social networking site where users connect and share content.
- **Sign-Up Form:** The interface for new account registration, which in this framework collects essential details including name, country code, phone number, Unique ID, gender, date of birth, nationality, and password.

Server Side Components:

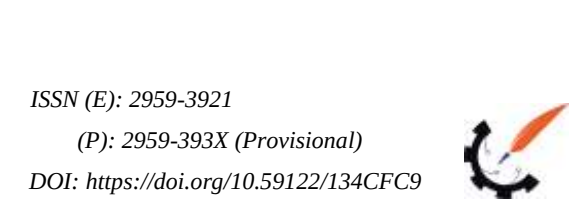
- **Facebook Server:** The central repository for storing and managing user account data.
- **Server-Side Authentication & Verification Module:** The core security component that validates user-provided information.
- **Addis Ababa City Digital Resident Database:** The official registry containing the digital residential information for all persons living in Addis Ababa.
- **Middleware:** System software that enables seamless integration and communication between the Facebook server and the external resident database, resolving issues of platform heterogeneity.

Authentication Process & System Responses:

- **Verification SMS:** A one-time password (OTP) sent to the user's registered phone number to confirm profile ownership as a final verification step.
- **Authentication Success (Ok):** A confirmation message returned if the user's provided personal information matches a record in the Digital Resident Database.
- **Authentication Failed:** An error message returned if the user's provided information does not match any record in the Digital Resident Database, preventing account creation.

Received: *19 March 2022;* ***Revised:*** *27 March 2023;* ***Accepted:*** *2 May 2023.* ***Published:*** *30 April 2023.*
Corresponding author- ***Basha Kesim***

ISSN (E): 2959-3921
(P): 2959-393X (Provisional)
DOI: https://doi.org/10.59122/134CFC9



Ethiopian International Journal of Engineering and Technology (EIJET)
Volume 1, Issue 1, 2023

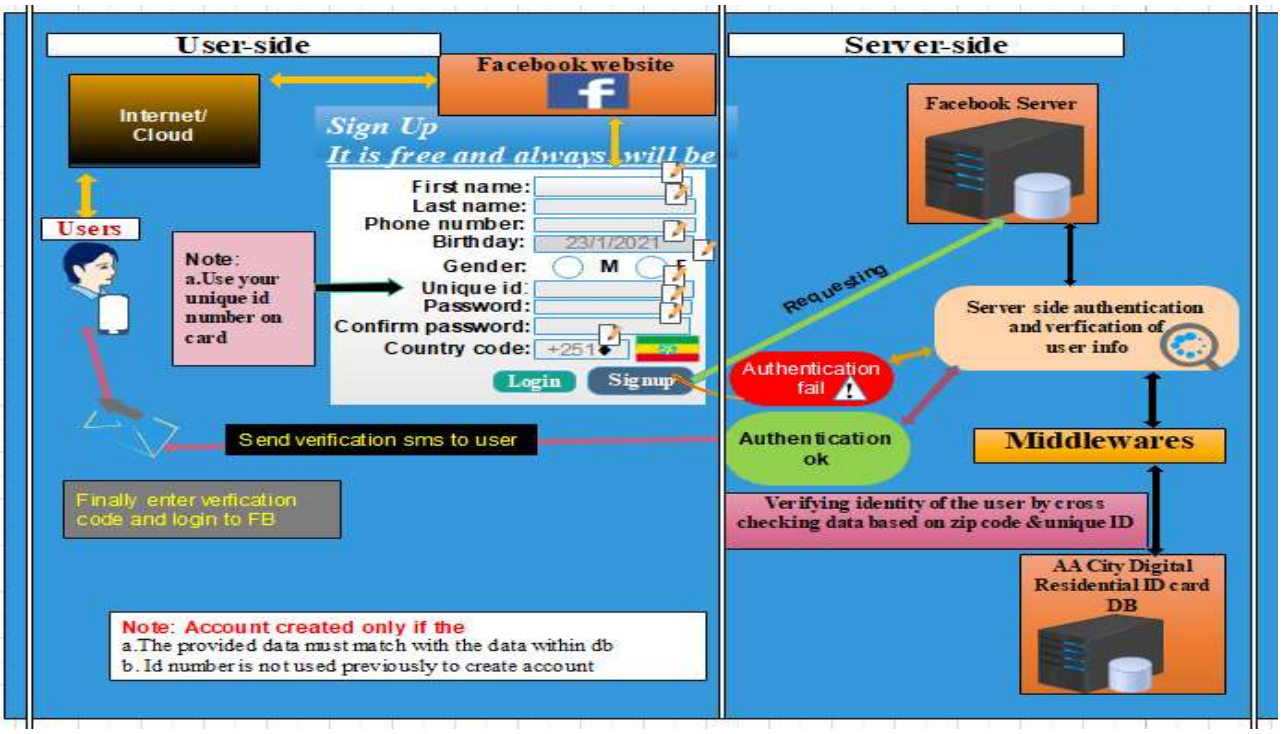


Fig. 16. Unique-ID-based cyber defense framework for enhancing the security of Ethiopian Facebook users.

Prototype Development

In this part, the developed system framework's functional prototype was presented. Fig. 16 shows the screenshots of the demonstrated prototype and Fig. 17 shows the Login page.

Design Description of a Prototype for Mobile Devices



Fig. 17: Facebook login through Mobile on Prototype

Received: *19 March 2022;* ***Revised:*** *27 March 2023;* ***Accepted:*** *2 May 2023.* ***Published:*** *30 April 2023.*
Corresponding author- ***Basha Kesim***

VII. Conclusion

The main objective of this study was to identify and analyze, from a security perspective, the deficiencies and challenges of the current state of social media, particularly in Facebook, and then develop a regulatory and control framework to improve the security checking technique for Facebook users. After primary data was collected using a survey and interview and analyzed together with secondary data, the researcher concluded that there are problems in Facebook user identity authentication and verification in our country and worldwide. Then the researchers' domain professional interview and social media users' survey responses concluded that the problems and challenges are destructive issues and require earnest and robust solutions by adding some functionality to the current Facebook user framework to save the generation from the act of unethical and malicious usage. The finding shows that the current Facebook user authentication and verification are vulnerable. They need strong attention to improve through scientific solutions. The current practices' challenges are identity theft, fake information dissemination, hatred of information propagation, impersonation, etc. In general, the recent Facebook security practices are found to be insecure. There is a lack of user identity proofing. It was used as the media in which fake accounts can be easily generated and used to disrupt society.

Based on the findings, the researcher designed the Unique-ID-based cyber defense framework for enhancing the security of Ethiopian Facebook users. The proposed Frameworks use a unique item or attribute representing only one person like the country code and UNIQUE ID number issued for the residents. This could be tremendous and significant to resolve the issues mentioned above and challenges with immediate effect on ground reality. Generally, this new framework that uses the unique user attribute, UNIQUE ID number on digital residential ID by the city and country code of the country, can restrict the user from creating a fake and duplicate account and impersonation problem via cross-checking the user-provided data with already stored data on the city database. The newly developed framework to enhance Facebook users' security by checking can do this task and ensuring that only verified users could be able to create an account and that user who provides unreal or fake information cannot create Facebook accounts. In the future, the researchers can focus their attention on user data security and privacy issue and come up with additional items that uniquely identify the users. Additionally, it is also recommended that upcoming researches have to focus on the more profound and broader inquiry of preventing identity theft happening by wrong Facebook users locally and worldwide.

Received: *19 March 2022;* ***Revised:*** *27 March 2023;* ***Accepted:*** *2 May 2023.* ***Published:*** *30 April 2023.*
Corresponding author- ***Basha Kesim***

References

1. A. G. D. S. Asres. K, "Automatic surveillance and control system framework-DPS-KA-AT for alleviating disruptions of social media in higher learning institutions," *Journal of Computer and Communications,* vol. 08, no. 01, pp. 1-15, 2020.
2. M. Smruthi and N. Harini, "A Hybrid Scheme for detecting fake accounts in Facebook," *International Journal of Recent Technology and Engineering (IJRTE),* vol. 7, no. 5, pp. 213-217, February 2019.
3. L.S. Wickramaarachchi, et al," Bio-metric social media network secure," *International Journal of Scientific and Research Publications (IJSRP),* Volume 6, Issue 4, April 2016.
4. D. Brian, "Social network usage & growth statistics: how many people use social media in 2020?," *Backlinko LLC,* August 12, 2020.
5. D. A. M, " Prevention technique for creating fake profiles and accounts on websites," *An international journal of advanced computer technology,* vol. VII, no. X, pp. 2826-2830 (5 Pages), 31 October 2018.
6. D. G. Yazan. B, "Integro: leveraging victim prediction for robust fake account detection in large scale OSNs," *Computers and Security,* vol. 61, pp. 142-168, 1 8 2016.
7. D. E. Katharina. K, "Fake identities in social media: a case study on the sustainability of the Facebook business model, "*Journal of Service Science Research,* vol. II, no. 4, pp. 175-212, 31 December 2012.
8. J. S. Memoona.S, "An automated framework for finding fake accounts on Facebook," *International Journal of Advanced Trends in Computer Science and Engineering,* vol. 7, no. 2, pp. 8-17, February 2018.
9. A. R. Gupta, "Towards detecting fake user accounts in Facebook," *SEA Asia Security and Privacy Conference 2017, ISEASP 2017,* vol. 1, pp. 1-6, 2017.
10. A. a. M. Mohammadreza.M, "Identifying fake accounts on social networks based on graph analysis and classification algorithms," *Security and Communication Networks,* vol. 1, no. 5923156, p. 8, 2018.
11. M. R. Fire, "Online social networks: threats and solutions," *IEEE Communications Surveys and Tutorials,* vol. 16, no. 4, pp. 2019-2036, 2019.
12. H., M. Meligy, "Identity verification mechanism for detecting fake profiles in online social networks," *I.J. Computer Network and Information Security,* vol. 1, pp. 1-3, 2014.
13. S. Kemp, "Digital 2020: Ethiopia", *Datareportal.Com,* 17 February 2020.
14. H. N. Sibhat, "Spreading Hatred a study of Facebook in Ethiopia," *Global Media Review (GMR),* vol. 1, no. 2, pp. 1-10, 2018.
15. M. Armstrong, "Social media reports," *statista.com,* Feb. 3, 2020.

Received: *19 March 2022;* ***Revised:*** *27 March 2023;* ***Accepted:*** *2 May 2023.* ***Published:*** *30 April 2023.*
Corresponding author- ***Basha Kesim***

16. H. B. C. A. K. G. Schroeter, "Creating safe and trusted social networks with biometric user authentication," *International Conference on Ethics and Policy of Biometrics.*, vol. 6005 LNCS, no. 03029743, pp. 89-95, 4 Jan 2010.
17. J. Nicas, "Why can't social networks stop fake accounts?", *The New York Times*, December 8, 2020.
18. Al Naqbi, N, Al Momani, N. Davies, "The influence of social media on perceived levels of national security and crisis: a case study of youth in the United Arab Emirates." *Sustainability*, 2022.
19. M. Tsikerdekis and S. Zeadally, "Detecting and preventing online identity deception in social networking services," *IEEE Internet Computing*, vol. 19, no. 3, pp. 41-49, May June 2015.
20. Amitvikram N, "Analysis of security and privacy issues in social media," *International Journal of Creative Research Thought*, 2022.

Received: *19 March 2022;* ***Revised:*** *27 March 2023;* ***Accepted:*** *2 May 2023.* ***Published:*** *30 April 2023.*
Corresponding author- ***Basha Kesim***