FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 9 No. 7, July, 2025, pp 119 – 125
DOI: https://doi.org/10.33003/fjs-2025-0907-3616

A FRAMEWORK FOR DEVELOPING SMART SOCIAL MEDIA PLATFORMS

***[1]Omogbhemhe Mike Izah and [2]Anthony Imhenkuomon**

[1]Department of Computer Science Ambrose Alli University, Ekpoma, Edo State, Nigeria
[2]School of Computer Science & Mathematics, Liverpool John Moores University, Liverpool, England

*Corresponding authors' email: mikeizah@gmail.com

ABSTRACT

Social media networks have revolutionized the activities of this age. Larger populations are using social media for education, exchange of ideas, business, marketing, fun, games, commerce and so on. However, there exists a fundamental challenge in this media, which is, the identity insincerity and theft. Users of social media create so many accounts for themselves and use these accounts for frauds. Some use other people information like names, pictures and profile to create multiple accounts for their dubious benefits. This has posed many fears on user not to believe in most media engagements. Connecting and communicating to some people in other locations of the world comes with a lot of doubt, fears and difficulties in exchanging business and expertise ideas which is one of the hallmarks of the social media. In dealing with these challenges, this paper has presented a framework for deploying smart social media platforms for enhanced information security and eliminating multiple opening/using of social media platform by same individual for fraudulent activities. This framework was developed using Object Oriented Methodology and C# was used to implement the prototype platform. Visual Studio was used as the IDE for the developed platform. The platform output shows its viability in preventing multiple account creation by users. The platform performance is shown in the implementation output of the system whereby the system will prevent the creating of multiple accounts and the use of other people information in creating a new account.

Keywords: Framework, Information Security, Social Media, Platform, Software

INTRODUCTION

The establishment of social media technology has led to the enrollment of a large number of network users into the global community. To a larger extent, these users are capitalizing on the benefits and available opportunities that this network carried. The improved computing power has therefore enhanced the freedom of interaction on social media that has made most users to freely share personal information via social media, carry out business operation with this media as well as storage of vital information in this media. Most organizations through social media use cloud computing to carry out most of their functions (Aggarwal, 2011). According to Abid, (2012), security, availability, and privacy are the topmost concerns in any cloud environment. Most users of social media are concerned much by the privacy of their information which can be easily compromised through data loss (Kumar and Lu 2010). The billion of information stored and process on this media raises problems related to data security that has prompted the need for maintaining personal data private and improvement of the trust towards the media. In most countries, it is a practice that internet fraudster open different social media account to perpetuate financial fraud on their victim with the aid of identity theft. Social networks provide an environment that is very much vulnerable to stealing and use of information from social media that is most sensitive (Chbeir and Bouna, 2013). During the early stages of Facebook development, for instance, access to social media information was easy due to lack of awareness by the users regarding privacy setting. Underdeveloped private policies and reliability to the common third party applications also contributed much to ease of access. Violations of privacy are of different magnitudes that vary right from image hacking, to profile hacking then later to the dangerous malware attacks. (Naif, 2016). Similarly, since anybody can open multiple accounts in social media without appropriate check, it is now a practice by many fraudster to hacking other people account and use the account for fraud without the person at the other end knowing that it is fraud. This has really discredited our identity by others in doing business with us as African. However, it is the view of this paper that the social media platforms can be made secured in eliminating identity theft.

Identity theft and related scams are a growing business for criminals. Unfortunately, social media and the increased availability of personal information have made these scams more common and easier to carry out. Removing yourself from all social media is drastic and challenging. Identity theft involves stealing or leaking of relevant data such as photos phrases or the use of one's information to come up with a new digital identity. With the use of phishing scams, individuals gain access to information via actions such as modification of addresses, getting the financial services or creation of new accounts using the victims' credentials. Some create fake documents and use it for their malicious gains (Buyya, Broberg and Goscinski, 2010). Identity theft and fraud are multi-billion-naira scams that impact large segments of the population. Identity theft can affect individuals and businesses in the following ways:

i. Identity theft can impact finances. The most noticeable impact of identity theft scams is financial. Depending on the scam's severity, attackers could empty bank accounts, take over investment or retirement accounts, and even potentially take control of a victim's mortgage. ID theft cases can necessitate legal services that further compound the financial impact.
ii. Identity theft can damage your career. Actions by scammers who misuse your identity could appear on background check and potentially affect employment opportunities.
iii. Identity theft can harm your reputation. Scammers could hurt your online reputation if they seize control of social media accounts. This is particularly damaging if you use social media for business. In worst-case scenarios, scammers could take control of a social media account and pose as the account holder while using the account

to distribute malware, send phishing emails, or launch additional attacks on other targets.

iv. Identity theft can lead to account bans. If identity thieves misuse your social media, platforms could ban your accounts. You could lose years of work spent building up a social media following.

Sen, (2013) opined that there are three major privacy issues that weaken the social media, these are; identity theft, profile hacking and bullying. Flowing from the above, it is clear that identity theft is a menace that must be address if the social media must achieve its benefits and full potentials. Hence the need for a better framework for curbing identity theft in Nigeria cannot be over emphasized. Social media is an emerging channel for marketing data, information and services around the globe. With this in mind of so many users, fake identity and fake services delivery have been recorded over the years as a result of these platforms (social media). Social media is the use of technology combined with social interaction to create value in the human ecosystem.

The evolution of this media has created a new paradigm of communication and interaction. It has become a part of our social life that helps us connect to friends, family, colleagues, or others. The advents of social media platforms like Facebook and Twitter have brought a revolutionary change in how we use the internet for personal and professional purposes. Social media has interestingly revolutionized the information and communication domain in the world (Ahmad , Ango and Barau, 2025). Social media is currently utilized both as broadcasting platform to amplify messages from traditional media sources (e.g., radio, television, print media) to demographics who are abandoning traditional broadcast technologies (e.g., telephones, television) and as an entirely new way of collaborating and co-creating content with target audiences (Malluhi, Shikfa, Tran and Trinh, 2019). Though this media came with alots of advantages, there exist a lot of challenges that needed to be taken care of if social media must attain its potentials. With over billions of users connected through online social network, it is important to consider the privacy and security of this platform in managing people's information. It's been noted that security concerns are very low on social media sites, hence the need for better models/framework in securing social media users. Researchers have provided series of methods that provides security to our social platform but these methods still comes with their own limitation of not taking care of identity information theft.

Distributed feature-based cryptography method was used by Yahiatene, Menacer, Riahla, Rachedi, and Tebibel, (2019) to provide privacy of data in online social network. The new framework was presented based on two main concepts, including cloud computing and feature-based cryptography. The cloud computing is used to store outsourced data by a third-party entity. By transferring data to this third party, data control is lost so no one knows where the data is stored. However the major limitation of this method is that there is no accurate data verification and matching with any existing platform before the processing is allowed on the media.

Bigwood, Rehunathan, Bateman, Henderson and Bhatti, (2008) introduced the Persona method. This method has the power of the user to divide friends into different groups. This method, like many methods, uses cryptography to maintain confidentiality. However, its only secures information during processing between two entities on the media but do not carry out any check before any information sharing can take place between these entities.

Raji, Jazi and Miri (2014) proposed a peer-to-peer social network architecture with privacy and data availability called PESCA. It is a distributed social network with privacy enabled for communication and data availability using diffusion encryption. In the same vein, the method does not provide opportunity of matching information with any trusted data management gateway before data processing is allowed. Li, Shen., He., Gu., Xu, and Xu, (2017) proposed a secure data sharing scheme for mobile cloud computing. The design uses feature-based encryption with encrypted text policy (CP-ABE) to control access. Their major feature of security is on the computing devices itself not the information provided. Wang, Ma, Luo and Gao, (2018) proposed a plan to increase the security and privacy of instant messaging for mobile social networking systems. This comprehensive plan for instant messaging security is based on Elliptic Curve Encryption (ECC) and Advanced Encryption Standard (AES). An offline key agreement process between users under the Daffy-Hellman (CDH) computational assumption is designed by short-term periodic key updates. The proposed scheme supports replay attack denial and counterfeit attack denial by using time labels and the Elliptic Curve Digital Signature Algorithm. (Hamideh, Behnaz, Elaheh and Behrou, 2023). Fugkeaw, and Fugkeaw and Sato (2018) proposed a special access control model with an effective key update function in the data outsourcing environment. This access control is based on combining feature-based encryption with encrypted text policy (CP-ABE) and role-based access control (RBAC). The proposed design is presented in the original CP-ABE design with the aim of improving the management of feature and key updates. In this scheme, the user key is included in the attribute certificate, which is used to decrypt the encrypted text with CP-ABE policy. If any changes include updating or canceling features that appear on the existing key, the key in the feature certificate (AC) will be updated as soon as access is requested. This significantly reduces the overhead of updating and distributing keys to all users simultaneously compared to existing CP-ABE plans (Hamideh et.al 2023).

Wang, Zhang and Zhang, (2018) provide a framework that includes IPFS decentralized storage system, atrium chain block, and feature-based encryption technology (ABE). Using this framework, the data owner has the ability to distribute encryption keys to data users and encrypt shared data by setting access policies, and this scheme provides precise access control over the data. This issue with this framework is that there is no hand shake between the system and any other valid system for data and processes authentication before and after operations in data handling is done. A fine-grained privacy control framework using searchable encryption was proposed by Chaudhari and Das, (2019). Search encryption in this scheme is based on a single keyword that is used for applications where multiple data owners upload their data to the server and then multiple users can access that data. This method uses feature-based encryption that allows the user to access any selected subset of data stored in the cloud without revealing their access rights to the cloud server. Hamideh et.al 2023 noted that Chen, (2020) proposed methods for sharing social data while maintaining safety in modern large social knowledge systems. In this way, by combining the concepts of information fragmentation with distributed system architecture, they improve traditional social data protection schemes and create a new social data protection scheme. In this proposed method, the protection of social images is used as the basis of the proposed scenario. In this method, two separate social platforms are used to protect the data. The cryptographic algorithm used in this method is of the selected cryptographic type. In this method, the images are protected into two small parts and the large public part is divided, the small part is stored in the first social platform and

the large part in the second social platform. When requesting access to this image, a user must receive both pieces from both social platforms. Zhang, Yao, Arthur, Weng, Liang and Su, (2021) proposed a novel blockchain-based privacy-preserving framework for online social networks, called BPP. Combined blockchain and public-key cryptography technique, the BPP framework can achieve secure data sharing, data retrieving, and data accessing with fairness and without worrying about potential damage to users' interest. Specifically, based on blockchain and public key encryption with keyword search technique, a secure, fair and efficient keyword search algorithm is proposed, with which the BBP framework realizes privacy preservation of user's query and then obtain accurate query results with assurance and without needing for any further verification operation in online social network (Hamideh et.al 2023).

MATERIALS AND METHODS

System methodologies are procedural steps embarked upon to design a system. This paper adopted the Object-Oriented Methodology. This helps in gathering adequate information on the requirements for the development of this framework. The prototype platform was developed using this framework. This platform helps to show how such system can easily navigate its operations to avoid multiple opening of social media platform by fraudsters. In the developed platform, ASP.NET was used to develop the active server pages and Cascading Style Sheet (CSS) was used to style the frontend. C# was used as the control mechanism of the platform while SQL Server provided the database. Visual Studio IDE was used for the full implementation and execution of the prototype platform. The SQL Server database was used as the relational database management system for both the social media server, proxy server and the National Identity System database prototype. All these act as the test-bed for the platform operations and to see how the platform achieve its objective of avoiding opening multiple social media page for same person. This help to bring sanity and authenticity to the media space.

The Proposed Framework

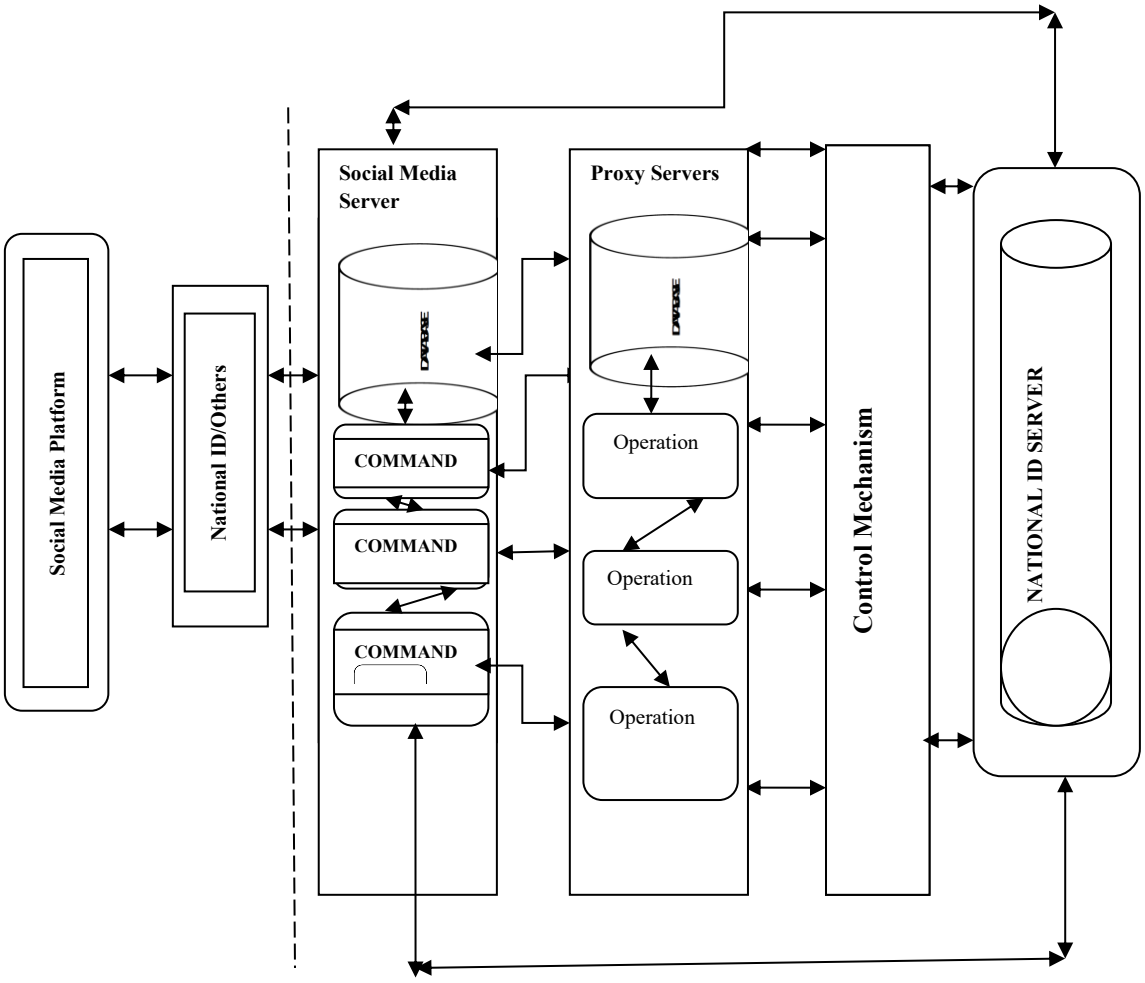

Figure1: Proposed Framework

Framework Description

The framework is made up of a series of entities that execute the structural process. Each of these entities has a series of tasks, behaviors, properties and directions. Four major entities, including social media servers, National Identification Server, Proxy server, and social media platform are used in this framework. Similarly, the framework algorithm is shown in table 1.

Social Media Server

The tasks of this entity include registering users, allocating storage space, creating an environment for sharing interests and data, communicating with other users, and searching for

users. Users communicate with their friends through this server. However, the information stored in this server during account creation must be generated from the NIS. This help to enforce strong security and to avoid creating multiple accounts for the same user.

National Identification Server (NIS)
This server is responsible for generating real identification information of the user using the NIN provided by the prospectus user of the media.

Proxy Server
In the proposed framework, there is a proxy server that plays the role of monitoring the activities/operations between the NIN and the media server. This help to create accountability in servers operations.

Media User Platform
This serves as an interface between the user and the database operations. In this framework, the user has limited activities to do when creating an account. However, after creating an account the user can use the media in accordance with the given privileges. The framework is smart because during the time of account creation, the user only provides his/her national identification number, username and password he/she intend to use in operating the media and the system is smart enough to generate all other needed information in order to avoid creating multiple accounts.

Algorithm 1: The framework algorithm

```
/* this algorithm is to use the ID to retrieve information for new account opening from Proxy Servers (National ID Server) */
Program Element (Input, Output);
Var A: Array[1……..?] of Integer;
/* Start Algorithm*/
Algorithm Search
Var I,N,X: Integer;
N: Total
X: Id
Found: Boolean;
Begin
I:=0;
Found False;
Repeat
        I:=I+1;
        Until (I>N) OR (A(I) =X);
If A(I)=X THEN
        Found:= True;
        WriteLn ("X is Found at Location at I:1 so Return All Needed Information of X);
Else
        WriteLn ("X is not Found so Return The person for National ID Registration);
End /* End If*/
```

RESULTS AND DISCUSSION
To show the workings of this framework, the platform was tested with user's data as shown in the figures below. It was observed that the platform could smartly have direct access to the National identity database to access the information of a prospectus user and if found that such users has existing social media platform, such registration will be denial. The different output/ screenshots of this platform operation are as shown in the figures below. Figure 2 is a sample of the first platform to sign in to the media. It requires the entry of the prospectus users NIN, username and password. When all these parameters are provided, the user will proceed to signup. Figure 3 shows exactly what happened if the NIN provided has already been used to register a user. This system is smart enough to prevent anybody creating multiple accounts because it will track such using the NIN as shown in figure 3 below. Similarly, figure 4 shows what will happen if the user is creating the media account with his or her NIN for the very first time. The system will track the details/information of the person from the NIN database and use those details to create an account. With this in place, the user can not supply false information to the media while creating an account. This will help to sanitize the media space of false or redundant information about the same person.

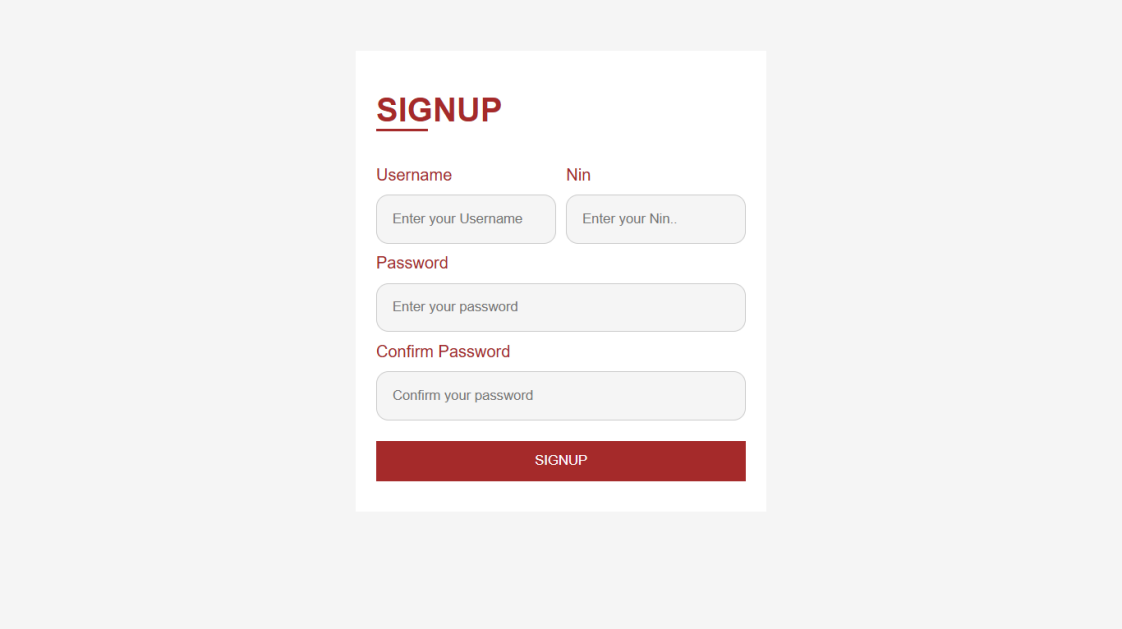

Figure 2: Smart Signup Page

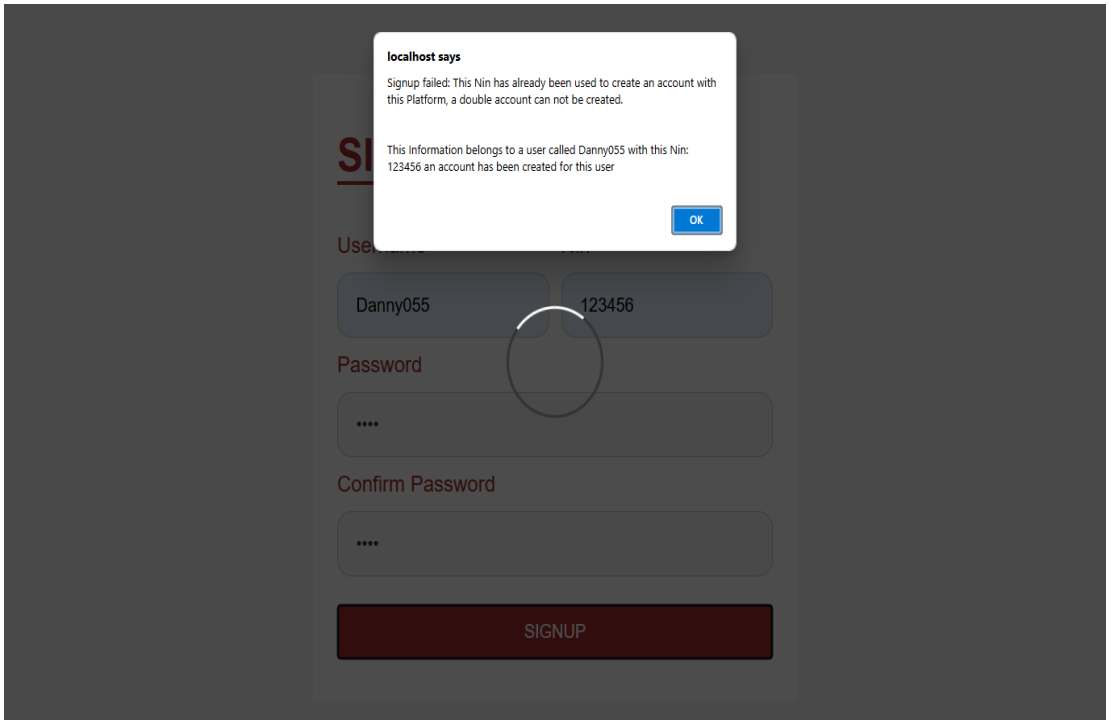

Figure 3: Screen output preventing multiple signup

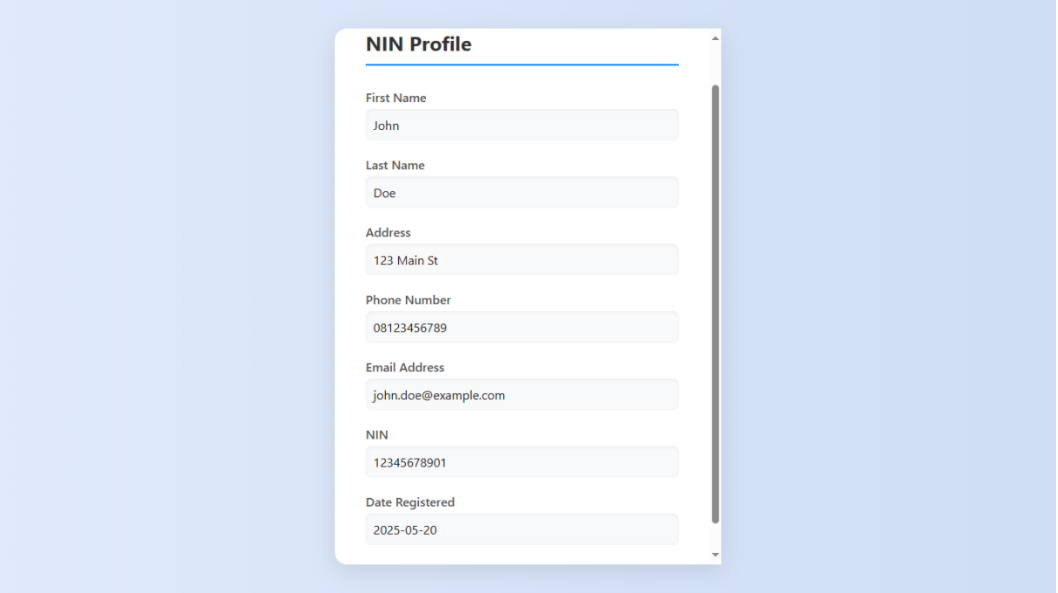

Figure 4: Successful Signin Output showing NIN information

CONCLUSION

The establishment of social media networks has provided some advantages to this age as well as some identity challenges. Social media is one obvious platform that many users believed that identity theft is common and find it difficult to fully believe its uses and operations. This paper has therefore provided a framework and a prototype platform that can be adopted in dealing with the issues of identity insincerity in the social media space/ platforms which will help to bring sanity to the system. The framework takes advantage of the national identification servers to track the real identity of an intended user and the operations/activities of all users. The framework provided in this paper can be fully developed as an API for social media platform. The full deployment of this framework will help to reduce if not eliminate internet frauds since users are only entitled to one account and their activities are been monitored by dedicated servers.

REFERENCES

Abid D (2012). Designing Network Services for the Cloud: Delivering Business-grade Cloud Services". Indianapolis, Ind: Cisco.

Aggarwal C.C (2011). An Introduction to Social Network Data Analytics, in Social Network Data Analytics. pp. 1-15. 2011. Springer US.

Ahmad M, Ango, A. K. and Barau, A. A (2025). Impact of Social Media Platforms on Farmers' Livelihood Assets in North-Western Nigeria. FUDMA Journal of Sciences (FJS). Vol. 9 No. 1 , pp 333 – 345. DOI:https://doi.org/10.33003/fjs-2025-0901-3143

Bigwood, G., Rehunathan, D., Bateman, M., Henderson, T. and Bhatti, S., (2008). Exploiting self-Reported Social Networks for Routing in Ubiquitous Computing Environments. In 2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (pp. 484-489). IEEE.

Buyya R, Broberg J and Goscinski A.M, (2010). Cloud computing: Principles and Paradigms. Vol. 87. John Wiley & Sons.

Chaudhari, P and Das, M. L. (2019). Privacy Preserving Searchable Encryption with fine-grained Access Control. IEEE Transactions on Cloud Computing, 9(2), 753-762.

Chbeir R, and Bouna B.A. (2013). Security and Privacy Preserving in Social Networks. Vienna: Springer.

Chen, X. (2020). Security-Preserving Social Data Sharing Methods in Modern Social Big Knowledge Systems. Information Sciences, 515, 404-416.

Fugkeaw, S., & Sato, H. (2018). Enabling Dynamic and Efficient Data Access Control in Cloud Computing Based on Attribute Certificate Management and CP-ABE. In 2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP) (pp. 454-461). IEEE.

Hamideh J, Behnaz M, Elaheh M, & Behrouz Z (2023). A Framework for Privacy and Security on Social Networks Using Encryption Algorithms. International Journal of Smart Electrical Engineering, Vol.12, No.1.

Kumar K, and Lu Y.H (2010). Cloud Computing for Mobile users: Can Offloading Computation save Energy? ", Computer, vol. 43(4), 51-56. 2010.

Li, R., Shen, C., He, H., Gu, X., Xu, Z., & Xu, C. Z. (2017). A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing. IEEE Transactions on Cloud Computing, 6(2), 344-357.

Malluhi, Q. M., Shikfa, A., Tran, V. D., & Trinh, V. C. (2019). Decentralized Ciphertext-policy Attribute-based Encryption Schemes for Lightweight Devices. Computer Communications, 145, 113-125.

Naif A.A (2016). Cloud Computing Privacy Concerns in Social Networks. International Journal of Computer (IJC) Volume 22, No 1, pp 29-36.

Raji, F., Jazi, M. D., & Miri, A. (2014). PESCA: A Peer-to-Peer Social Network Architecture with Privacy-Enabled Social Communication and Data Availability. IET Information Security, 9(1), 73-80.

***Sen J (2013). Security and Privacy Issues in Cloud Computing Architectures and Protocols for Secure Information Technology Infrastructures", 2013, pp.1-45.

Wang, Z., Ma, Z., Luo, S., & Gao, H. (2018). Enhanced Instant Message Security and Privacy Protection Scheme for Mobile social Network Systems. IEEE , 6, 13706-13715.

Wang, S., Zhang, Y., & Zhang, Y. (2018). A Blockchain-Based Framework for Data Sharing with Fine-Grained Access Control in Decentralized Storage Systems. IEEE 6, 38437-38450

Yahiatene, Y., Menacer, D. E., Riahla, M. A., Rachedi, A., & Tebibel, T. B. (2019). Towards a Distributed ABE Based Approach to Protect Privacy on Online Social Networks. In 2019 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-7). IEEE.

Zhang, S., Yao, T., Arthur Sandor, V. K., Weng, T. H., Liang, W., & Su, J. (2021). A Novel Blockchain-Based Privacy-Preserving Framework for Online Social Networks. Connection Science, 33(3), 555-575.