Modeling Authentication Mechanisms on Social Media Accounts

Prof. Prachiti Deshpande
Professor, Department of Computer Engineering,
B.D.C.E Wardha India
prachitideshpande@gmail.com

Article Info
Page Number: 102 – 104
Publication Issue:
Vol 71 No. 1 (2022)

Article History
***Article Received**: 18 November 2021*
***Revised**: 03 December 2021*
***Accepted**: 19 December 2021*
***Publication**: 28 January 2022*

Abstract

Fake pages are used to exploit important categories, by using personal photos or personal information, in order to spread lies and discredit. This is illegal and threatens privacy. So, dealing with social networking sites has become a dangerous and risky thing. Hence, each important category seeks to have its pages on social networks distinctive and authenticated in order to attract real followers, in addition to removing all fake pages that use the name or pictures in order to mislead the followers. The authentication mechanisms on social media accounts differ from one site to another, but they are similar in terms of the objective, which is authenticating personal pages, in addition to showing a logo that distinguishes these pages from other pages. This mechanism requires everyone to follow specific procedures to complete authentication. Hence, obtaining a trust logo is not easy, accompanied by complicated procedures that are difficult to follow by normal users, unlike the important personalities who usually have managers who maintain their daily work and accounts.

Keywords: - Modeling, Authentication etc.

Introduction

Social networking sites can interact with the other person at any time wherever via electronic platforms [1, 2]. The lack of confidence in dealing seriously with most users comes from the frequency of creating accounts usually for entertainment, but over time, there has been increased interest in verifying the identity of the real owners of accounts. The reason for the emergence of fake pages for users is usually to spread rumours and false news or the theft of followers [3]. It has become necessary to have a mechanism that is able to authenticate accounts on social networks. Some social networking sites have created mechanisms to limit the fake pages, or show a logo that distinguishes the real pages, enabling followers to identify the real pages of the personalities who wish to follow them. Facebook, Twitter and others have also used Blue Check, a blue sign on their personal pages. These mechanisms and procedures are specific only to specific categories (media, sports, government, etc.), which have greatly reduced the problems they were directing, reducing fake pages that spread news and rumours. In order to obtain this blue sign, a number of documentary paperwork must submitted to confirm the identity of the page owner [4].

Moreover, the existing method is effective only for specific categories, and its procedures are rather complex in order to verify and authenticate personal identity. Most users cannot authenticate their pages, for a number of reasons, including that the procedures for getting the blue check are somewhat complex and require time. The authentication depends on the number of followers, which prioritizes accounts with greater influence, as followed by the Twitter company. Hence, this study seeks to find a technical and free mechanism to authenticate the social networking pages, through the integration of Blockchain technology with social networks [5].

One way to improve these sites is to take advantage of Blockchain features and the tools it provides to document and verify personal information. It will help in reducing the complex procedures used in social networks, in order to authenticate accounts and confirm the real information of account holders. This verification is usually displayed as a logo shown on the personal pages as a blue check, the mark indicates that it's a reliable page. The use of the new technique will enable users to approach social networks more confidently without concern. As a result, the code that refers to the block containing the real information will become a sign that enables followers to confirm that the personal page is real and reliable, to allow social networks to focus on the goals for which they were created, such as social communication. This research aims toward the goal that authentication pages be available to everyone without conditions or restrictions to obtain a sign of trust (code block) on social media pages.

Methodology

In the model, it is necessary to have information stored in the form of a block for the service applicant to be distributed. All users of block chain, on the other hand, approved it having an effective account on the social network, and then the account is linked with the service applicant block to be a trusted reference stored in block. In other words, the information is authenticated in a participatory manner from both sides of the block and social page.

Results and Discussion

In the proposed model, the following steps are required for account authentication: Create an account on the social network, complete the registration of all personal information, create a block in block chain which contains all the personal information of the service applicant (personal photos, documents, links. etc). The fourth step is to add the personal account link in the block, distribute the block chain on ledgers and receive the block receipt notice, get a hash code in the block that contains all the personal information, which is the reference number, through which it becomes the address where the personal information is matched with the account. The seventh step is to add the hash code to the personal page on the social networking page and the appearances of block chain logo and the hyperlink to the block containing the documented information.

At the end, the page containing the block chain logo and the hyperlink becomes reliable based on the information stored in the block distributed to everyone. Hence, the aim is to give confidence to the social media pages based on information previously stored in the block and distributed on the ledger. This authentication is difficult to falsify, modify or violate because any process carried out on block notifies everyone in the books to get approval for any action.

One account and one block only, in other words, and this research deals with the possibility of linking one account with one block. In the future we may add additional options or the possibility of linking more than one account in a block.

The number of pages documented using the blockchain is expected to increase because of its ease as well as being a successful alternative to authenticate, and confirm the identity of account holders and reduce the fake pages. Anyone can easily check through the hash code on a personal page and then match it with the personal information in the block. On the other hand, the effectiveness of the proposed mechanism does not require papers, i.e. the traditional way through official government documents in order to ascertain the identity of a service applicant. The role of social networking is expected to be limited to social networking, a focus on the social objectives for which it was created and give a third-party opportunity to document personal pages.

Conclusion

In summary, this research provides a model of an effective technical mechanism capable of electronic authentication using the block chain, in order to be a substitute for the authentication mechanisms used in social networks and to create a secure environment that all users can handle safely and confidently. The proposed model uses the trust algorithm of the blockchain. This model relies on creating trust by distributing the stored block of personal information to all ledgers. This block is encrypted and does not accept modification or deletion, hence the block becomes a reference to verify personal information stored in the block which is then linked to the personal information in the social media account. The result is a hash code that appears on the profile page, through which any follower can compare the information stored in the block with the information shown on the account. If there is a match, the account is authenticated, and the reverse is false. This research contributes significantly to authenticating social media pages, finding technical alternatives to reduce the risks faced by social media users, as well as highlighting the possibility of adding third parties to reduce the number of fake pages, and create a safe environment.

References

[1] Marcelo Maia, Jussara Almeida, Virgílio Almeida, "Identifying User Behavior in Online Social Networks", Proceedings of the first Workshop on Social Network Systems, 1 April 2008

[2] Michael Fire,etc,(2014)"Online Social Networks: Threats and Solutions," IEEE Communication Surveys & Tutorials, Vol. 16, No. 4, Fourth Quarter 2014

[3] Mohammad H. Allymoun, Nidal F. Shilbayeh, Sameh T. Khuffash, Reem Al-Saidi (2014). Protecting the Privacy and Trust of VIP Users on Social Network Sites, International Journal of Computer, Information, Systems and Control Engineering, Vol. 8 No.9, 1419-1429

[4] Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing,and privacy on the Facebook. In P. Golle& G. Danezis (Eds.), Proceedings of 6th Workshop on Privacy Enhancing Technologies (pp. 36-58). Cambridge, UK: Robinson College

[5] Krishnan, S. ., and D. B. . Prasanthi. “Prediction of CPU Utilization in Cloud Environment During Seasonal Trend”. International Journal on Recent and Innovation Trends in Computing and Communication, vol. 9, no. 12, Dec. 2021, pp. 08-11, doi:10.17762/ijritcc.v9i12.5493.

[6] Devmane, M., & Rana, N. (2013). Security Issues of Online Social Networks. Advances in Computing, Communication, and Control, Springer. pp. 740-746

[7] Hussain Bukhari, S. N. . (2022). Data Mining in Product Cycle Prediction of Company Mergers . International Journal of New Practices in Management and Engineering, 10(03), 01–05. https://doi.org/10.17762/ijnpme.v10i03.127