

## AN ENHANCED AUTHENTICATION SCHEME FOR PREVENTING PHISHING ATTACKS ON WHATSAPP ACCOUNTS

**Jumoke Soyemi<sup>#</sup> & Mudasiru Hammed<sup>\*</sup>**

Department of Computer Science, The Federal Polytechnic, Ilaro.

[#jumoke.soyemi@federalpolyilaro.edu.ng](mailto:#jumoke.soyemi@federalpolyilaro.edu.ng); [\\*mudasiru.hammed@federalpolyilaro.edu.ng](mailto:*mudasiru.hammed@federalpolyilaro.edu.ng)

### Abstract

WhatsApp has recently become the most popular among the social media platforms because of its multimedia capability to support multiple, video, audio, graphics, texts and others. Thus, making it attractive for use by several organizations and Institutions as a means of official communication. This popularity gained also made it attractive to phishers, attackers and hackers, creating another major concern for users. Although, the recently updated WhatsApp platform now has a two-step verification scheme to enable a good security measure; however, the recent activities of hawkers with their continuous penetrations on this platform informed this paper to propose ahead of time a two-way authentication scheme augmented with typing rhythm modelled with integer programming. The proposed authentication scheme, when implemented, will provide more secure and efficient security for this platform peradventure the present two-step verification scheme is bridged.

**Keywords:** Integer programming, Hackers, Two-way authentication scheme, Typing Rhythm model, WhatsApp

### Introduction

The advent of internet technology brought about several innovations in communication including social networking media, online banking among others, thus making networking and communication much more accessible, not only for individuals but also for organizations and Institutions (Gupta, Arachchilage, & Psannis, 2018). Presently, social networking platforms have risen to become one of the most popular media of sharing information and communication (Mao, Tian, Li, Wei & Liang, 2017). The internet-enabled mobile phones have also helped the popularity of these social networking media (Soyemi, Oloruntoba & Okafor, 2015) tremendously. The usefulness of some of these platforms spanned beyond just staying in touch with friends but also in research exploration, collaborations and academic activities (Mao, Tian, Li, Wei & Liang, 2017). Therefore, social networking media can be conceived as nodes representing individuals or organizations (Bilge, Balduzzi, M., Balzarotti & Kirda, 2011) with the nodes connected via friendship, business associations, ideas, visions, common values and general interest.

The existence of social networking has been around for a while, but the internet-enabled social networking became popular in recent (Kelly, Kerr & Drennan, 2010). Business organizations are now finding solace in social networking media such as LinkedIn, Facebook, Myspace, Instagram, Twitter and WhatsApp to mention a few. The popularity of these media among internet users are on the rise because of the benefits they offer (Bilge, Strufe, Balzarotti & Kirda, 2009), having millions of registered users across the globe sharing and communicating with ease (Kelly, Kerr & Drennan, 2010). Aside from sharing and communication, activities such as entertainment, e-commerce, delivering teaching materials are also carried out through these platforms.

However, certain people across the globe have taken advantage of the anonymity provided by the media to fool individuals with fake offers, or by misrepresenting themselves as legitimate (Shah, Trevathan, Read & Ghodosi, 2009). This act is referred to as phishing which is a kind of email or contact spoofing fraud attempts that target individuals and members of a specific organization, seeking authorized access to confidential data.

Phishing attacks are not typically initiated by “random hackers” but are more likely to be conducted by perpetrators for financial gain, trade secrets, or military information (Nelson, Lin, Chen, Iglesias & Li, 2016). Different studies have proposed different anti-phishing strategies to reduce social networks challenges, but literature revealed that WhatsApp security challenges had not been dealt with. The focus of this study is phishing attack in WhatsApp where hackers often invade the WhatsApp group and tempt group of users to provide their confidential information such as credit card details, bank account details, and secret number or password. In some cases, hackers will trick users into visiting fraudulent links or websites. They normally use the medium when there are a significant fraction of end clients that operate without a robust security mechanism. This study used a Two-factor authentication scheme augmented with typing rhythm modelled with integer programming. The proposed authentication scheme is quite efficient for securing social network attacks.

Akram & Ko (2014), presented a framework for end-to-end security and privacy of mobile chat services and associated requirements. The study identified that a multitude of social media services have converged on smartphones and that, with the increasing interconnectivity, the use of online services is posing a massive security threat to users of such services. Dashtinejeg (2015) identified security services for instant message applications and designed an architecture for an end to end encryption of mobile messaging applications to secure and ensure their privacy. Frauenstein and Flowerday (2016), identified the serious behavioural priming that made users susceptible to social engineering attacks and elaborated on activities engaged by users that leads to such attack. Rastogi and Hendler (2017) argued that the signal protocol forming the basis of WhatsApp version 2.16.2 end-to-end encryption released in April 2016, cannot preserve the privacy of users. The study examined the security architecture of WhatsApp and performed analysis on the various protocol used and made the submission that there is some metadata unencrypted within the application that are prone to attack.

Shirvanian, Saxena & George (2017) exposed the key weaknesses in the security and usability of the code verification methods employed in the remote end to end encryption applications. The study Pointed out the poor security and the fundamental severe vulnerability of internet-based communication applications. Krapta, Shyry & Krishna (2019), proposed the use of single secret key generated from both the sender and the receiver which must not be communicated through other channels in addition to the existing end-to-end encryption system that can easily be compromised. Still, integrity must be validated in periodical intervals. Although this method is suitable, hackers and attackers are also using tricks to get such secret keys. Agrawal *et al.* (2019) only discussed how WhatsApp uses end-to-end encryption technique with different protocols for privacy and security purposes. However, studies have established the fact that end-to-end encryption is not secure enough for privacy and protection. Wong, Supian, Ismail, Kin & Soon, (2001) identifies that “typing biometrics that analyzes the rhythm or behavioural pattern of a user at a keyboard could be used as a means of identifying users”.

Li, Sancherz & Hua (2016), in their study on WhatsApp security analysis, pointed out that “the major concern observed, which is the issue of WhatsApp’s session establishment. They established that after a session is first initialized between two users, the same session is used for all subsequent interactions between the two, barring an external change like app uninstallation/reinstallation or a device change, leaving the system vulnerable to Man In The Middle attacks, which are extremely dangerous”. Although WhatsApp offers a Key verification, because this is not mandatory, users are at risk if they reply on the Trust on First Use principle that is inherent in session establishment. The study concluded by proposing a simple verification step before session creation to confirm that the connection is authentic.

Rösler, Mainka & Schwenk (2018) explained that the investigation of end-to-end protected group communications had gained only a little attention despite the fact that one-to-one communication of secure instant messaging applications has been in the focus of recent researches in Frosch *et al.* 2016; Cohn-Gordon, Cremers, Dowling, Garratt & Stebila, 2017; Kobeissi, Bhargavan & Blanchet, 2017). The study, therefore, provided a security model and a methodology for analyzing group instant messaging protocols and the study claimed that the underlying model is of generic purpose and could be applied to other secure group instant messaging protocols.

In this study, however, beyond the end-to-end encryption of two-way authentication scheme, that has been discovered to be porous and not secure, typing rhythm, modelled with integer programming is employed to enhance the security mechanism of this social media and in this wise, WhatsApp social media platform.

## **System Design and Architecture**

### **Existing Architecture**

The architecture in figure 1 shows an existing two-factor authentication scheme used as a means of authentication. The Architecture was built with a Trusted Platform Module (TPM), which is a chip that can securely store artefacts for platform authentication purposes. A PIN generated by the system was also used for the subsequent user login. However, the problem with this existing system is that, in Trusted Platform module, programs on the chip can be rewritten for malicious activities (information insertion). It may be difficult for the system to detect such malicious activities, and the system can also authenticate an adversary as a legitimate user. The major aim of the two-factor authentication scheme is to use “What the user knows and what the user has”.

The proposed system in this study aside from using “What the user knows and what the user has” added “what the user is”, that is user’s typing pattern (typing rhythm) to enhance the security mechanism for WhatsApp account. This will drastically remove the security challenges of a WhatsApp account.

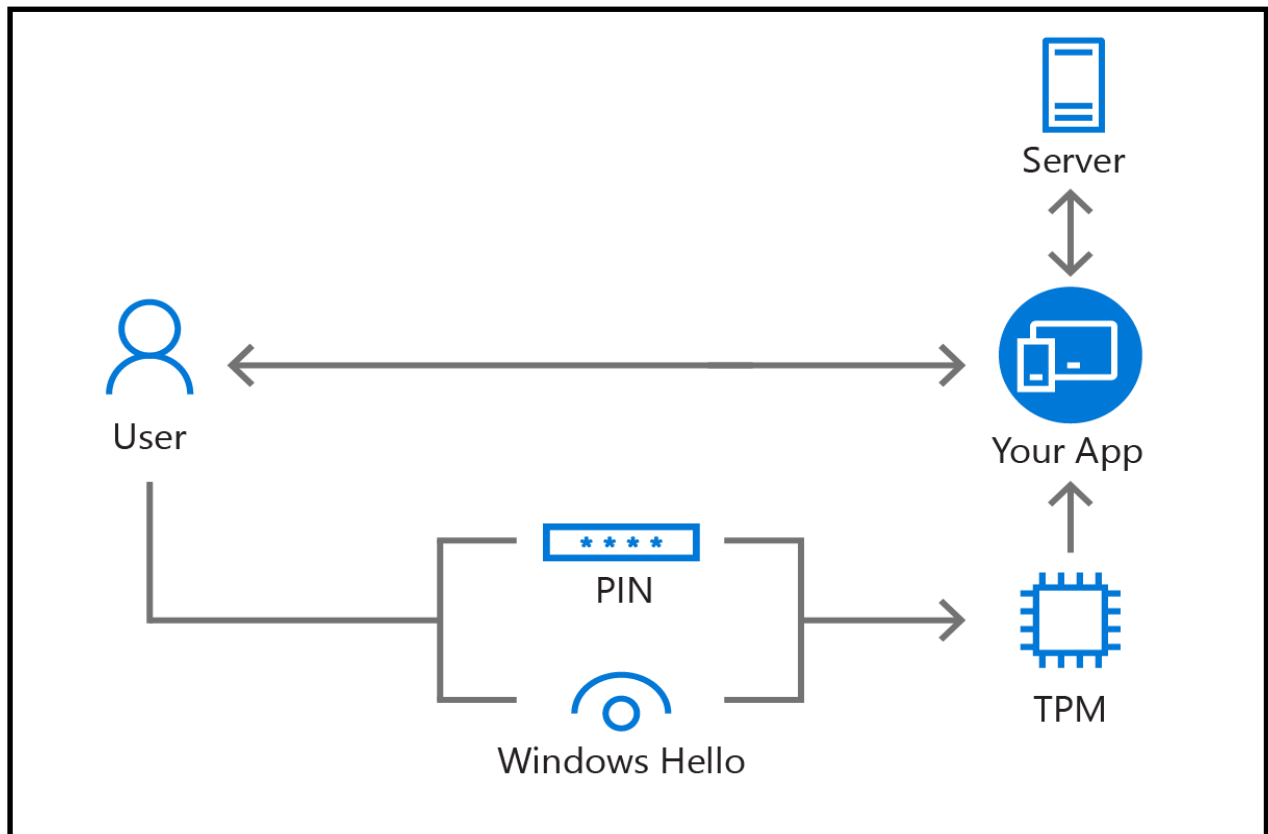


Figure 1: Existing System Authentication Architecture (Microsoft, 2016)

### Proposed System Architecture and Design

For the system design, typing rhythm technique is used, that is, Personal Identification Number (PIN), which consists of different characters with an extra dimension of typing dynamics. It is not only that an intruder must know the correct PIN, but he or she must also be able to replicate the rate of typing and time intervals to gain access to the system (Dahalan, Salami, Lai & Ismail, 2004; Wong, Supian, Ismail, Kin & Soon, 2001). The proposed system design model in figure 2 is made up of two phases which include: Registration and Login phases. The Pseudocode of the proposed model is also captured in figure 3.

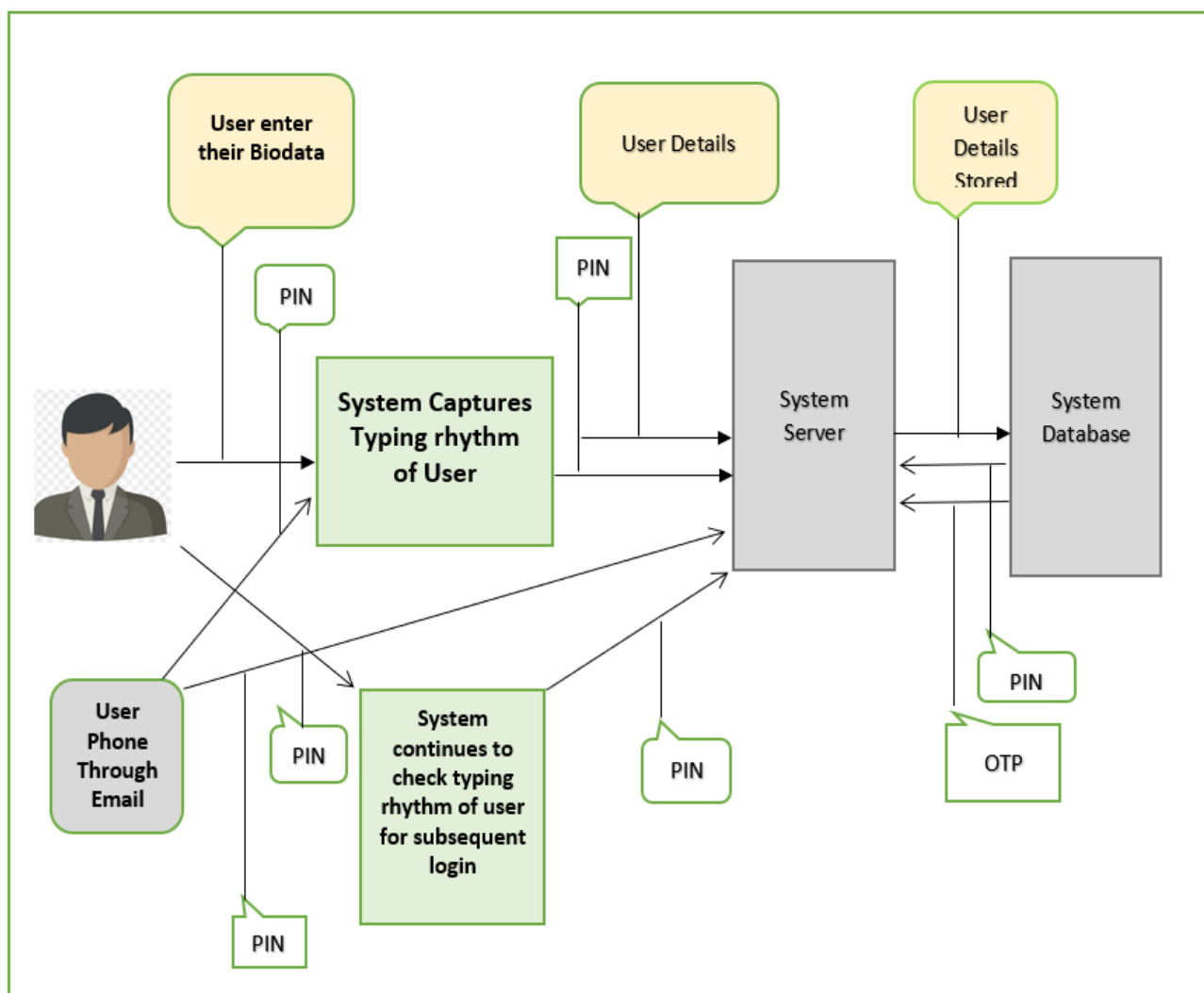


Figure 2: Proposed Enhanced Authentication Model

*Step 1: Input user's details*  
*Step 2: Generate Personal Identification Number (PIN)*  
*Step 3: Input the PIN three times*  
*Step 4: Capture the typing rhythm of the user (time spent to enter the PIN)*  
*Step 5: Login with the PIN*  
*Step 6: Check if the PIN and the typing rhythm match*  
*Step 7: Grant Access if there is a match*  
*Step 8: Deny access if otherwise*

Figure 3: Pseudocode for the Model Generation

During the registration phase, the WhatsApp users will register with details such as name, age, sex, home address, phone number and email address which the system will use as a unique identifier. Once all the information is submitted to the system, the information will be stored in the system database where a template will be generated for individual user's information. After the user's details are stored in the database, the system will pop up a dialogue box for the user to enter the desired PIN and once the user clicks on the submit button. The system does not only store the PIN, but it will also store the time taken by the user to type and submit the PIN and the process will be repeated two more times to confirm if a user enters the same PIN. The rule is that user must enter the same set of the PIN with a combination of different characters and the time taken in entering

the PIN for the last time must be less than the second time and the time taken for the second time must be less than the time taken the user to enter the PIN for the first time.

Mathematically,

$$\text{Maximizing WhatsApp server Operating System (OS)} = \sum_{ij=1}^3 A_i T_j \quad (1)$$

$$\text{Subject to} \quad A_1 \leq T_1 \quad (2)$$

$$A_2 \leq T_2 \quad (3)$$

$$A_3 \leq T_3 \quad (4)$$

$$T_3 \leq T_2 \leq T_1 \quad (5)$$

$$\text{Constraint} \quad T_1, T_2, T_3 \leq 0 \quad (6)$$

The study used equation 2 to model the user's first attempt for entering his/her PIN and time taken the user for the attempt. Equation 3 modelled a second attempt and time taken while equation 4 modelled the third attempt and time taken the user to complete the action. If the proposed system must work correctly, then, equation 5 must be satisfied. However, the system stores the time taken by the user to complete the third attempt during registration as a maximum number of times that a user can spend to complete access to the system in the subsequent login. A user can use less than the time spent for the third attempt during registration, but a user cannot spend more than the time stored for the third attempt during registration.

The time spent for the third attempt has been stored, subsequently, whenever the user wants to login into the system, the time spent must be less than or equal to the time stored by the system. In a situation where a user wants to login into the proposed system and more time is spent than the time stored in the system during registration, even though the PIN is correct, the user will be deactivated. The system will allow the user to login again, but this time, the user must spend less time than the time spent for the first attempt, and the user will be logged out after the third attempt. That is, each time a user wants to login into the proposed system, the system will first check the number of times that the system stored for the user's third attempt during registration and compare it with the time that user spent on the current attempt, to determine whether the user will be activated or deactivated. If the time spent on the current attempt is greater than the time spent on the third attempt, the user will be deactivated, and the user will be activated otherwise. If a user is able to get One Time Password (OTP) to login into the proposed system, the PIN and the time stored for the third attempt during registration must be satisfied. That is, an intruder must not only know the correct PIN using the system, but he or she must also be able to replicate the rate at which the PIN must be typed. Once the user's PIN is validated and the time spent is satisfied, the OTP will be generated and sent to the user's email address, and once the entering of OTP is correctly done, the user will gain access to the proposed system. This means that, not only that an intruder must know the correct password using this technology, but must also be able to satisfy the typing rhythm of the legitimate user.

## Conclusion

WhatsApp among other notable social networking platforms has been identified to stand out among equals in its ability to handle both Organizational and Institutional information, leading to several of such sectors approving it as a medium for official communication. The need to take immediate action on the recent security issues of phishing and the activities of hackers before it is too late informed this study and the proposal here. The use of Two-factor authentication scheme augmented with typing rhythm modelled with integer programming when implemented will make the WhatsApp platform better secured against attackers. Their recent activities show that in no recent time, they might be able to break the current two-way verification scheme presently operational on the WhatsApp platform and would be a disaster to wait till then before researchers begin to investigate the possible means of strengthening and tightening up the security measures that will make the platform stringent enough against such attacks.

## References

Agrawal, M.R., Rathore, M.R., Jain, M.S., Yadav, S.M., Singh, M.V., Mishra, M.Y., & Singh, N.P. (2019). Case Study on Whatsapp end to end Encryption. *International Research Journal of Modernization in Engineering Technology and Science*, 2(4), 1266-1271.

Akram, R. N., & Ko, R. K. (2014). End-to-end secure and privacy preserving mobile chat application. In *IFIP International Workshop on Information Security Theory and Practice* (pp. 124-139). Springer, Berlin, Heidelberg.

Bilge, L., Balduzzi, M., Balzarotti, D., & Kirda, E. (2011). A summary of two practical attacks against social networks. In *Trustworthy Internet* (pp. 171-185). Springer, Milano.

Bilge, L., Strufe, T., Balzarotti, D., & Kirda, E. (2009). All your contacts belong to us: automated identity theft attacks on social networks. In *Proceedings of the 18th international conference on World wide web* (pp. 551-560).

Bonneau, J., Anderson, J., & Danezis, G. (2009). Prying data out of a social network. In *2009 international conference on advances in social network analysis and mining* (pp. 249-254). IEEE

Cohn-Gordon, K., Cremers, C., Dowling, B., Garratt, L., & Stebila, D. (2017). A formal security analysis of the signal messaging protocol. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 451-466). IEEE.

Dahalan, A., Salami, M. E., Lai, W. K., & Ismail, A. F. (2004). Intelligent pressure-based typing biometrics system. In *International Conference on Knowledge-Based and Intelligent Information and Engineering Systems* (pp. 294-304). Springer, Berlin, Heidelberg

Frauenstein, E.D., & Flowerday, S.V. (2016). Social network phishing: Becoming habituated to clicks and ignorant to threats?. In *2016 Information Security for South Africa (ISSA)* (pp. 98-105). IEEE.

Frosch, T., Mainka, C., Bader, C., Bergsma, F., Schwenk, J., & Holz, T. (2016). How secure is TextSecure?. In *2016 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 457-472). IEEE

Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*, 67(2), 247-267

Kelly, L., Kerr, G., & Drennan, J. (2010). Avoidance of advertising in social networking sites: The teenage perspective. *Journal of interactive advertising*, 10(2), 16-27

Kobeissi, N., Bhargavan, K., & Blanchet, B. (2017). Automated verification for secure messaging protocols and their implementations: A symbolic and computational approach. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 435-450). IEEE

Krapta V., Shyry, S.P. & Krishna, M.R. (2019) WhatsApp Encryption – A Research. *International Journal of Recent Technologies and Engineers (IJRTE)*, 8(2s3), 522-523.

Li, C., Sanchez, D., & Hua, S. (2016). *WhatsApp Security Paper Analysis*. Tech. rep. Massachusetts Institute of Technology.

Mao, J., Tian, W., Li, P., Wei, T., & Liang, Z. (2017). Phishing-alarm: Robust and efficient phishing detection via page component similarity. *IEEE Access*, 5, 17020-17030.

Microsoft (2016). Convenient two-factor Authentication with Microsoft passport and windows hello. Retrieved from:

<https://blogs.windows.com/windowsdeveloper/2016/01/26/convenient-two-factor-authentication-with-microsoft-passport-and-windows-hello/>

Nelson, J., Lin, X., Chen, C., Iglesias, J., & Li, J. J. (2016). Social engineering for security attacks. In *Proceedings of the The 3rd Multidisciplinary International Social Networks Conference on Social Informatics 2016, Data Science 2016* (pp. 1-4)

Rastogi, N., & Hendler, J. (2017). WhatsApp security and role of metadata in preserving privacy. *arXiv Prepr. arXiv1701*, 6817, 269-275.

Rösler, P., Mainka, C., & Schwenk, J. (2018). More is less: On the end-to-end security of group chats in Signal, WhatsApp, and Threema. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 415-429). IEEE.



Shah, R., Trevathan, J., Read, W., & Ghodosi, H. (2009). A proactive approach to preventing phishing attacks using Pshark. In *2009 Sixth International Conference on Information Technology: New Generations* (pp. 915-921). IEEE.

Shirvanian, M., Saxena, N., & George, J. J. (2017). On the pitfalls of end-to-end encrypted communications: A study of remote key-fingerprint verification. In *Proceedings of the 33rd Annual Computer Security Applications Conference* (pp. 499-511).

Soyemi, J., Oloruntoba, S. A., & Okafor, B. (2015). Analysis of mobile phone impact on student academic performance in tertiary institution. *International Journal of Emerging Technology and Advanced Engineering*, 5(1), 361-365.

Wong, F. W. M. H., Supian, A. S. M., Ismail, A. F., Kin, L. W., & Soon, O. C. (2001). Enhanced user authentication through typing biometrics with artificial neural networks and k-nearest neighbor algorithm. In *Conference Record of Thirty-Fifth Asilomar Conference on Signals, Systems and Computers*, 2, 911-915, IEEE.