A CRITICAL REVIEW ON USE OF IOT IN STUDYING SOCIAL BEHAVIOR

Dr. Sanjay Kumar, Professor, Department of Computer Science & Engineering, Galgotias University

ABSTRACT

The extensive integration of smart mobile devices to the Internet of Things (IoT) applications means that a lot of valuable information is found in users' mobile device use, interactions with other devices, and movement patterns. This significant body of data may be efficiently utilised to authenticate a user's identity if monitored over a period of time. Biometric features, such as fingerprints and irises, have effectively increased the security of access in prior works. Behavior-based identification is nevertheless developing as a revolutionary idea in the integrated social networks and IoT infrastructures with its adoption on smart portable devices. We provide an intelligent add-on to assist with continual verification of users in this article. Data collected from built-in sensors and statistics for social networking apps on mobile devices are used in the tests. As part of the data collection process, features are assembled together over time and evaluated using machine learning algorithms. Our analysis demonstrates that when devices with continuous verification intelligence are enabled, users can only be rejected a false 10% of the time, and they are not interrupted during biometric authentication the other 90% of the time. The suggested approach has up to 97% success ratio in the event of unusual behavioural patterns by using an aggregated behaviour pattern on five distinct social networking sites.

KEYWORDS: IOT. SOCIAL BEHAVIOT, TECHNOLOGY

INTRODUCTION

GPS, camera, accelerometer, gyroscope, and microphone are among several sensors included in modern mobile devices like smartphones and tablets. In light of the growing interest and appeal of these devices, they have been established as possibilities for integration into IoT-based sensing applications. the major components of IoT are discussed in the following two points: 1) sensor hardware, and 2) middleware software to serve as a communication platform among multiple system components, 3) processing of data, and 4) data storage. Wearer and handheld devices have had computing resources like as CPUs, memory, and data storage compact enough to be incorporated into them .

With the recent advancements in Internet of Things (IoT), particularly with the dramatic increase of smartphones, continuous authentication on individualised devices is now achievable. Self-tracking systems utilising multiple sensor types, like smartphones with sensors that monitor various facets of roadway conditions, such as road condition for smart transportation, public safety, and emergency preparedness, can support a constant flow of data about conditions like roadway conditions that can be applied to all kinds of transportation systems. Given the large number of IoT devices that are being used, the utilisation of them as a starting point for user verification is projected to increase. At the same time, the incentives need to be sufficiently effective in order for the users to provide their mobile devices as a service. Now that we have smartphones, tablet computers, and watches, we can now access social networking services that are available on the web through mobile apps. Every day more and more portable devices are on the market, which has enabled the massive popularity of social networking sites (SNS) to continue to grow. Social networking services (SNSs) are used by about seven out of ten persons in the U.S. Ericsson studied the apps for social networking and found that mobile apps generated an extraordinary amount of data that could be enhanced with analytics to better serve many organisations. Classifying the data types in into six groups as stated in the following five categories of data: service data, disclosed data, entrusted data, incidental data, and derived data Most users exhibit habitual behaviours that are modifiable, which enables ongoing behavioural recognition, as described in. According to this assumption, we performed an investigation on social media mobile devices by concentrating on ongoing behavioural patterns on mobile social networks and verifying that cellphones were being used by the owners. For this purpose, we have developed a mobile behavioural analytics framework to evaluate social activities, and have included social activities metrics to build user signatures. This biometric approach depends on identifying a person based on their unique characteristics, such as a fingerprint, iris, or face, and then classifying patterns from these traits to identify or enable access to a user or a group. This kind of identification is often once-and-done, and confirmation needs regular engagement.

BEHAVIOR STUDY

Behavioral analytics is a technology that predicts how mobile users will behave based on their smartphone behaviours. continuous authentication of a user is possible on a personal device because of the behavioural features of mobile users. A plethora of mobile apps are available for today's intelligent gadgets. Social networking applications have grown from important to an indispensable aspect of everyday life. Social network companies get large amounts of data sent to and from its users. Social networks are a valuable source of rich data. These may be used to detect different sorts of relationships. There are a lot of examples, such as the online student-supervisor cooperation information produced in or the buddy rating application established in, of how great new student-supervisor online collaboration ideas are.

An essential and fundamental necessity for ensuring privacy is proper user identification and authentication. Password and pin codes are often used as a means of authentication in cellphones, however they don't provide adequate security, and users have to memorise several sets of passwords or pin codes for each phone. To further strengthen security, fingerprint and facial recognition are included into certain smartphones to eliminate the need to memorise passwords. An identifying method based on physiology is called physiological identification, whereas an identification method based on behaviour is called behavioural identification. Those functions use just the device-dependent parts of face, voice, and fingerprint identification and need pricey processing units. Also, constant identification which is based on human habitual patterns, such as typing, walking, conversations, and social interactions, is non-intrusive and is performed through identifying characteristics such as typing walking social interactions, and communication. Social biometrics are described as identifying an individual user in diverse social environments by means of communication and interaction patterns. An online or offline environment may be a venue for a social event, which is either referred to as the "cyber world" or the "physical world." Online interactions happen when someone is blogging, using social media, and has Internet connection. Behaviometrics (currently developing) claims to give a cost-effective option that maintains security while also being more economical.

To maintain device level security of mobile smart devices, especially when they are recruited for IoT-driven sensing, we provide an intelligent approach. In order to be able to understand the patterns of smartphone users and extract characteristics from smartphone sensors and social network interactions, the suggested system is based on online behavioural analyses of mobile users using smartphones. Using real data spanning many months, this suggested technique is tested and evaluated. The functionality in the study covers data location, session frequency, length, and number of users from multiple social media sites using a mobile device. In preliminary work on disrupting users' authentication on mobile devices in the face of spoofing attempts was described. This study makes substantial progress in research on system performance by considering both normal and abnormal settings. The contextual weighting elements are further discussed, and their empirical investigation is included.

CONCLUSION

Because the Internet of Things allows users to use their own personal devices in sensor campaigns, they may also engage in participatory or opportunistic sensing. Authenticity is essential for proper operation of these gadgets because of the following reasons: Rejection rates that are higher than the service can handle may cause biometric authentication, which might de-incentivize the usage of built-in sensors. Conversely, acceptance rates that are too high can indicate unreliable sensor data. A Social Internet of Things (SIX) made up of people, objects, services, and online interactions has emerged due to convergence of IoT and social networks. It has several advantages, including the ability to find one's way around, increased scalability of services, and increased trustworthiness of acquired data. This article has explored continuous verification in SitoT, where smartphone social network data and user behavioural variables are compiled to form online reputation scores for each user. A continuous verification method has been described, one that relies on social behaviour measurements from a sample of users. We have used authentic traces that have been gathered over a prolonged period of time.

REFERENCES

1. Bashir, U., Jha, K. R., Mishra, G., Singh, G., & Sharma, S. K. (2017). Octahedron-Shaped Linearly Polarized Antenna for Multistandard Services Including RFID and IoT. *IEEE Transactions on Antennas and Propagation*, *65*(7), 3364–3373.

https://doi.org/10.1109/TAP.2017.2705097

2. Charoenpanyasak, S., Sasiwat, Y., Suntiamorntut, W., & Tontisirin, S. (2017). Comparative analysis of RFID anti-collision algorithms in IoT applications. *2016 International Symposium on Intelligent Signal Processing and Communication Systems, ISPACS 2016*. https://doi.org/10.1109/ISPACS.2016.7824757
3. DeMartino, C. (2016). Wireless technologies flood the IoT landscape. *Microwaves and RF*, *55*(5), 70–72. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84998775217&partnerID=40&md5=cbe99fac5a3c3105f63b97ca09b4fc2e
4. Fan, K., Liang, C., Li, H., & Yang, Y. (2014). LRMAPC: A lightweight RFID mutual authentication protocol with cache in the reader for IoT. *Proceedings - 2014 IEEE International Conference on Computer and Information Technology, CIT 2014*, 276–280. https://doi.org/10.1109/CIT.2014.80
5. Hanel, T., Bothe, A., Helmke, R., Gericke, C., & Aschenbruck, N. (2017). Adjustable security for RFID-equipped IoT devices. *2017 IEEE International Conference on RFID Technology and Application, RFID-TA 2017*, 208–213. https://doi.org/10.1109/RFID-TA.2017.8098883
6. Michta, E., Szulim, R., Sojka-Piotrowska, A., & Piotrowski, K. (2017). IoT-based flood embankments monitoring system. In R. R. S. Linczuk M. (Ed.), *Proceedings of SPIE - The International Society for Optical Engineering* (Vol. 10445). SPIE. https://doi.org/10.1117/12.2280830
7. Petracca, M., Bocchino, S., Azzarà, A., Pelliccia, R., Ghibaudi, M., & Pagano, P. (2013). WSN and RFID integration in the IoT scenario: An advanced safety system for industrial plants. *Journal of Communications Software and Systems*, *9*(1), 104–113. https://doi.org/10.24138/jcomss.v9i1.162
8. 85062942572&partnerID=40&md5=82aca5b6254ea6c5d214d08f61aa85d3
9. Valente, F. J., & Neto, A. C. (2017). Intelligent steel inventory tracking with IoT / RFID. *2017 IEEE International Conference on RFID Technology and Application, RFID-TA 2017*, 158–163. https://doi.org/10.1109/RFID-TA.2017.8098639
10. Zeb, S., Satti, J. A., Habib, A., Amin, Y., & Tenhunen, H. (2017). Dual-polarized data dense chipless RFID tag towards IoT applications. *2017 International Symposium on Wireless Systems and Networks, ISWSN 2017*, *2018-Janua*, 1–5. https://doi.org/10.1109/ISWSN.2017.8250038