International Journal of Engineering & Technology, 7 (3.28) (2018) 275-277

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Smart Bicycle Sharing System for Non-Commercial Purposes using Time-based One-Time Password Algorithm

Husna Humaira Abu Backer Sidek, Azrul Amri Jamal*, Mokhairi Makhtar, Syed Abdullah Fadzli

Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Besut, Terengganu, Malaysia
**Corresponding author E-mail: azrulamri@unisza.edu.my*

Abstract

Bicycle sharing systems have been accepted openly by the public. Many developed countries prepared some kind of bicycle sharing system in order to advocate exercising and promotes healthy living. Nevertheless, these systems are usually for commercial purposes and required the user to pay some amount of money to use the service. This paper discusses regarding smart bicycle sharing system designed for non-commercial use, such as in universities, schools, or small villages where the bicycle sharing service are to be given out to users without a fee. At the same time, the whereabouts and availability of the bicycles should be managed carefully in order to avoid losing the bicycles. Several one-time password algorithms have been studied and the most suitable algorithm has been used to generate a 6-digit code in order to unlock bicycles from its bicycle stations. The system is designed to be as easy to use as possible, and with an acceptable amount of security.

Keywords: *Bicycle Sharing; One Time Password; Security; Embedded Programming; Information Systems.*

1. Introduction

Bicycles have several advantages over other modes of public transportation for short-distance urban trips. They neither create air nor noise pollution in their operation, and they generally do not add to vehicular congestion. Bicycles are not commonly thought of as a form of public transportation. Nonetheless, recent technological advances have allowed this to be successfully challenged throughout the world with the bicycle sharing technologies. The basic premise of the bicycle-sharing concept is sustainable transportation and this technology promotes healthy lifestyles and sustainability among commuters, casual riders, and tourists.

The evolution of bicycle sharing technologies and business models has led to a range of options for program implementation. For instance, Mexico City one of the most congested cities in the world, implemented bicycle sharing as a way to help reduce traffic congestion. Despite historically low cycling levels, this program has reached capacity of 30,000 users [1]. This shows that, given appropriate chance and trust towards communities, bicycle sharing idea can be accepted, utilised, and cultivated in community and can soon become a norm in everyday life.

2. Smart Bicycle

A Smart Bicycle allows individuals to meet their transportation needs in an environmentally sound manner [2]. Bicycle sharing is a flexible form of personal public transport. With a smart card or other form of identification, a user can check out a bicycle from a station, use it for a short ride, and return it to any other station [3]. Smart Bicycles are ideal for short-distance urban trips due to their advantages over other types of public transportation. Smart Bicycle provide on-demand transportation, require less infrastructure than other modes of transportation and do not create pollution in their operation [2].

The central pillar of modern systems, the bicycle sharing scheme which has no fixed docking station is having major issues where people keep bicycles longer than the allowed period. Despite of these technologies, there continue to be bicycles that are parked indiscriminately, which causes obstruction or inconvenience to the public such as users of wheelchairs and other personal mobility aids and this cannot be easily integrated into Institute of Higher Learning.

Unfixed stations lack the flexibility to meet the needs of students who make quick and short-distance trips. Some experts say that's largely because many cities were not designed to be bicycle friendly. Despite the fact that the popularity of the bicycle sharing systems is rising, there are some drawbacks. The bicycle sharing programs have the potential for being abused, which has been proven by recent vandalism and theft in Paris. Approximately, 9,000 bicycles were lost or damaged in the past year alone [4]. In this research, a smart bicycle sharing system which has fixed docking station is essential to meet the needs of the modern college student.

3. Password Securing the Bicycles

Considering the Smart Bicycle that are to be proposed will be targeted towards students inside a campus, a reasonable level security for the bicycles is needed. Among security algorithms that being considered are the One Time Password (OTP), HMAC based One Time Password (HOTP) and Time-based One Time Password (TOTP). One of these algorithms will be utilised to generate a password to be used for the unlocking mechanism of the smart bicycle sharing system.

3.1. One Time Password

OTP is an instant password. In other words, it is a code that changed after every time we use it to authenticate [5]. OTP are passwords that are only valid for a single or small number of transactions. An OTP is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords [6]. They are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will be no longer valid. OTP generation algorithms typically make use of pseudo randomness or randomness. This is necessary because otherwise it would be easy to predict future OTPs by observing previous ones.

3.2. HMAC-based One Time Password

The authors in [7] define HOTP as an HMAC-based One Time Password technique. The HOTP algorithm is based on an increasing counter value [5]. Both the client and server will typically have a counter value. Server generates the password to use the counter. If both passwords match, the server authenticates the user and updates the counter (increment/ decrement the counter), it may happen that the counter at client and server may drift (due to passwords generated by client but not submitted, or passwords submitted by client but does not reach to server due to network failure, etc.). In this case will response to server with denial service. In [7], the researchers have provided the output of the HMAC − SHA − 1calculation in 160 bits, they have to truncate this value to something that can be easily entered by a user.

$$\mathrm{HOTP}(K, C) = \mathrm{Truncate}\big(\mathrm{HMAC} - \mathrm{SHA} - 1(K, C)\big)$$

where truncate represents the function that converts an HMAC − SHA − 1 value into an HOTP value. The Key (*K*), the Counter (*C*), and Data values are hashed high-order byte first.

3.3. Time-based One Time Password

The TOTP Algorithm is an extension of HOTP Algorithm that uses time as the moving factor [8]. Time dynamism is an OTP generation principle widely utilized in two-factor authentication (2FA) schemes. Two-factor authentication usually referred to a two-step of verification. It's a security process which the user provides two authentication factors to verify they are who they say they are. A different password is needed for different time to prevent number of attacks, this schema depends on two periods, static period is designed for user to input the OTP into the login form upon receipt of the dynamic period password, and the length of which can always be customized by the client [9].
Basically, TOTP is defined as TOTP = HOTP (K, T) where T is an integer present time, k present secret key. The current time present initial time for the user login.

$$T = \left\lfloor \frac{(current\ time - T_0)}{X} \right\rfloor$$

X represents the time step in seconds (default value *X* = 180 seconds) and is a system parameter. T_0 is the UNIX time to start counting time steps (default value is 0).

3.4. Suitable OTPs for Bicycle Sharing System

To meet those requirements for this project, comparison is necessary in order to choose which one is the best technique. This will include an advantage, why TOTP and a table of comparison.

3.4.2. Advantages of TOTP

The benefit of using time based instead of a counter is that it continually changes and gives new values automatically. An OTP usually remains valid for a given time period. The authentication server performs the same computations as the user and since they share the same secret and current time, the codes will be identical. A power of TOTP is that it does not need any form of network connectivity to generate new codes. As long as the clock of the device is partially in synchronization with the rest of the world, it's going to keep generating a valid OTPs.

3.4.2. Disadvantages of TOTP

TOTP is vulnerable to time-manipulation attacks. The combination of secret key and timestamp generates always exactly the same token result. Allowing internal clock manipulation weakens the entire concept, possibly leading security problems. If the internal clock was moved back on a device, the 6-digit codes from earlier would become valid again.

Table 1: OTP Algorithm Comparison

Factor	OTP Algorithms		
	HOTP	TOTP	OTP
Replay Attack	Prevent	Prevent	Prevent
Speed	Slow	Fast	Medium
Duration of OTP	Long	Short	Long

3.4.2. Choosing between Algorithms

The main difference between HOTP and TOTP is that HOTP key can be valid for an unknown amount of time. Whilst, TOTP key keep on changing and only valid for a certain amount of time. Due to this difference, TOTP is considered as a more secured One-Time Password solution for the system. This is done in order to avoid users booking the bicycle long before they are planning to use it, making the bicycle unavailable for others to use.

4. Developed Program

4.1. Smart Bicycle Sharing System Framework

Smart Bicycle Sharing System consists of two main parts: servers; and bicycle station. These two parts are connected via internet and each of them has their own role in the whole system. The servers is where all the web servers and database servers are placed. The web servers provide a user interface for users to interact with the system in order to check out the bicycle. The database servers are used to store all of the bicycle sharing transactions, where all the data can later be extracted and put in reports for management to analyse. The 6-digit TOTP codes are generated here to suitably utilise the processing power of the servers.
The second part of the system is the bicycle stations. These bicycle stations consists of a microcontroller controlling and collecting inputs from the user and bicycles. Keypads are used to retrieve the TOTP codes to be sent to the microcontroller to check its validity. Radio-frequency identification (RFID) readers are used to sense whether there are any bicycles parked at the bicycle stations.
In practice, there are only one server are needed to control multiple bicycle stations. The servers will share the TOTP codes with the microcontroller at the bicycle stations, instructing them to open bicycle locks according to the user-selected bicycle. Figure 1 shows the framework of the smart bicycle sharing system.

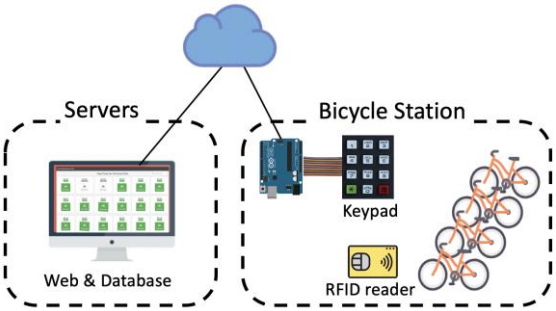

Fig. 1: Smart Bicycle Sharing System Context Diagram

4.2. Registration

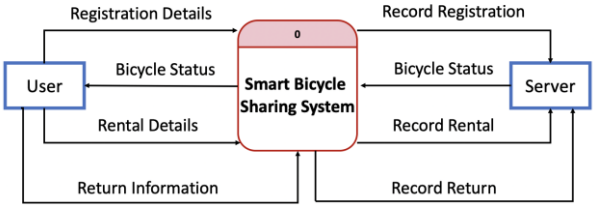

Fig. 2: Smart Bicycle Sharing System Context Diagram

Figure 2 shows the context diagram of the Smart Bicycle Sharing System that has been developed. The user would be required to register their information first onto the system. Among information that are needed during the registration is name, address, matriculation number, scanned copy of matriculation card, and identification card. Once the registration is completed, the user will be able to check the real-time availability of the bicycle to be borrowed (Figure 3).

4.3. Real-time Bicycle Selection

Fig. 3: Bicycle Availability and Selection User Interface

User can select any available bicycle to borrow from the system. This feature will let the users choose if they have any preferred bicycle to be borrowed. From here, users are brought into the TOTP authentication workflow, as shown in Figure 4.

4.4. TOTP Authentication

Once a bicycle is selected, the system will generate a 6-digit TOTP code and is then shown to the user. The user then remembers the code and goes to the bicycle stations to key in the TOTP code there. The TOTP code that has been entered will be compared with the code in the system. The chosen bicycle will be unlocked once a correct TOTP code has been entered. User can borrow the bicycle, and once the RFID tag on the bicycle is not detected, the system will consider that the bicycle has been disengaged from the bicycle station, thus being borrowed. The bicycle is then registered as borrowed and the information will be delivered to the main sharing system to let others know that the bicycle is not available for borrowing.

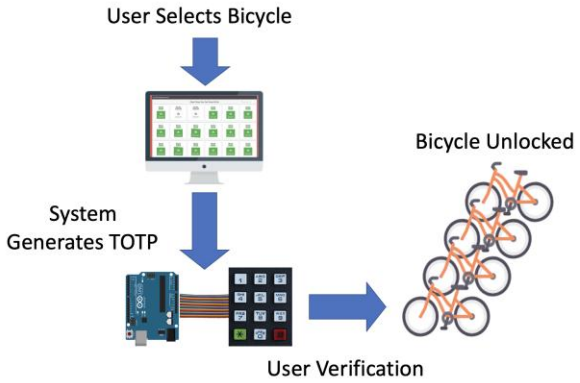

Fig. 4: TOTP Authentication Workflow

4.5. Returning the Bicycle

When the user has finished borrowing the bicycle, the user can put the bicycle at any smart bicycle sharing system stations that are unlocked. When the bicycle stations detect the RFID tag of the bicycle nearby, it automatically informs the system. The system then registers the return action and automatically locks the bicycle at the returned location. This action completes the whole borrowing process and the whole process is stored in the database as bicycle sharing history.

5. Conclusion

The bicycle sharing system that being proposed is suitable for bicycle sharing in a closed community such as the university, and schools where the community trusts each other and only requires suitable amount of security features. The implementation of TOTP in the system is suffice in order to detect and control, which bicycle has been used by the user.

Acknowledgement

The authors would like to express their gratitude towards Universiti Sultan Zainal Abidin for preparing a conducive environment for research and development, and for providing financial support in publishing this article.

References

[1] Shaheen, S., & Guzman, S. (2011). Worldwide bikesharing. ACCESS Magazine, 1(39), 22-27.
[2] DeMaio, P., & Gifford, J. (2004). Will smart bikes succeed as public transportation in the United States? Journal of Public Transportation, 7(2), 1-15.
[3] Gadepalli, S., Kost, C., & Schroeder, B. (2012). Public cycle sharing systems: A planning toolkit for Indian cities. https://3gozaa3xxbpb499ejp30lxc8-wpengine.netdna-ssl.com/wp-content/uploads/2014/07/Public_cycle_sharing_toolkit_ITDP_121204.pdf.
[4] Scott, M. https://www.criticalcycles.com/blogs/blog/16490364-the-pros-and- cons-of-bike-sharing.
[5] Lee, S. J., Lee, J. S., Lee, M. K., Lee, S. J., Choi, D. H., & Kim, D. K. (2011). Low-power design of hardware one-time password generators for card-type OTPs. ETRI Journal, 33(4), 611-620.
[6] Kalaikavitha, E., & Gnanaselvi, J. (2013). Secure login using encrypted one time password (OTP) and mobile based login methodology. International Journal of Engineering and Science, 2(10), 14-17.
[7] Hoornaert, F., Naccache, D., Bellare, M., & Ranen, O. (2005). HOTP: An HMAC-based one-time password algorithm. https://tools.ietf.org/html/rfc4226.
[8] Tokula, U. I., & Esiefarienrhe, B. M. (2015). Design and implementation of a two-factor, one time password authentication system. International Journal of Computer and Organization Trends, 5(6), 1-4.
[9] Ren, X., Wu, X. W., & Tang, K. (2012). TSPass: A dynamic user authentication scheme based on time and space. International Journal of Computer Science and Network Security, 12(10), 45-53.