2016 IEEE International Conferences on Big Data and Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Computing and Communications (SustainCom)

Secure Bike Sharing System for Multi-modal Journey

Mohammad Shahriar Rahman
KDDI R&D Laboratories, Inc.
Saitama, Japan
Email: mohammad@kddilabs.jp

Shinsaku Kiyomoto
KDDI R&D Laboratories, Inc.
Saitama, Japan
Email: kiyomoto@kddilabs.jp

***Abstract*—Bike sharing systems (BSSs) are getting popular in many cities of the world as an integrated part of multi-modal journey due to its flexibility and eco-friendly nature. Future BSSs will have a pool of Internet of Things (IoT)-integrated smart bikes with computation and communication capabilities. Such systems will be able to provide the service providers with real-time and non-real-time information about user demands, bikes and environments for improved quality of services. However, manipulation of logistics data (e.g. showing availability of bikes or parking where none may exist) and mobility operations (e.g. unauthorized tampering with service-related data) may disrupt the whole service. This paper proposes a framework for secure bike sharing service under multi-modal journey environment using symmetric key encryption and digital signature. Our proposal lets a service provider to collect information from stations and external service providers, and communicate with users in a secure way so that the user gets correct information and a quality service. The proposed framework has the potential to offer enhanced quality of service through security features compared to existing systems for multi-modal transport users.**

KeyWords: Bike Sharing System, Multi-modal Journey, IoT, Security

I. INTRODUCTION

Attention on intelligent transport systems as a sustainable solution has been accelerated in recent days due to its impact on reduced energy consumption and environment pollution. Bike Sharing Systems (BSS) are one of the major components of intelligent transport systems in smart cities. A numerous number of cities around the world offers bike sharing (BS) service with thousands of bikes available for sharing. BSS increases flexibility for commuters by allowing convenient access (e.g., pick up or drop off a bike at any station) to on demand-based rides fo their daily life. The success of a BSS significantly depends on this flexibility [1].

To ensure a user-focused and robust service, BSSs should be a part of multi-modal journey environment [2] such that a user can plan her whole journey conveniently. BSS should offer services (e.g., cycle availability, reservation) to both bike users and Bike Sharing Service Operators (BSSOs) (e.g., bike distribution service, empty or overfilled station monitoring and management). BSSOs need to overcome a number of challenges in bike distribution and multi-modal service integration. User demand is typically unpredictable, and may fluctuate throughout a day due to factors like weather conditions, city events, traffic conditions, and so on. All these factors lead to an imbalanced distribution of the bikes over time and space. Sensor-integrated smart bikes, along with their users' sensor-rich internet-enabled smartphones, will enable loT(Internet of Things)-integrated BSSs [3]. IoT-integrated BSSs using physical as well as participatory sensing (PS) can provide BSS-related information including real-time information about the users' mobility patterns and demands.

Security of Bike Sharing Services

Security of a bike sharing service for multi-modal journey is important due to the nature of service and its impact on overall transport management. Manipulation of logistics (e.g. showing availability of bikes or parking where none may exist) data and mobility operations (e.g. unauthorized tampering with service-related data) may disrupt the whole service. If a user receives falsified information (due to adversarial attacks), then there is a high probability that she arrives at an empty bike station when starting the trip, or to an overfilled bike station when returning the bike. These situations will delay operations and create a bad customer experience. Also, mobile applications often log location information which may be stored insecurely. For example, traffic information and navigation services are often provided in exchange for collecting location, speed, and other information that is used to improve the quality and coverage of the service provided [4]. However, if the service provider has no security policy, then sensitive bike user data may be compromised, or the service itself may be manipulated (e.g. showing traffic congestion where none may exist). Authentication is important because parties (i.e., users and service providers) to communicate must also trust that they are speaking to a legitimate counterparty, rather than a third party that may be masquerading as the communication partner. Data transmitted can be captured by a third party that situates itself between two parties in the communications media. For bike sharing services, the integrity and confidentiality of services for road users are important. Bike user's integrity focuses on the integrity of data being stored in bikes or other connected IoT devices. User authentication controls are designed to verify an identity to process ticketing, reserving, parking services. User's privacy policies should obfuscate data to preserve the confidentiality of user data that may be fraudulently used for other purposes by an attacker. Such private data may include origin and destination location, route, speed, and other data generated by journey planning systems,

978-1-5090-3936-4/16 $31.00 © 2016 IEEE
DOI 10.1109/BDCloud-SocialCom-SustainCom.2016.71

bikes or connected devices. On the other hand, bike service or external service operators may collect traffic, weather, parking, and multi-modal connections data, and may further process and package various information for dissemination to various communication channels (e.g. other service provider partners). Security controls must be applied to ensure the authenticity, integrity and confidentiality of information to ensure that correct data is exchanged among authentic operators so that users do not get misinformed. Moreover, service providers need to authenticate the identity of the other party before transmitting data to prevent the disclosure of data.

Our Contribution In this paper, we propose a secure bike sharing system. The proposal consists of two algorithms. The first algorithm allows a user to reserve a bike and parking space according to her journey plan (immediate or future) through her multi-modal journey planning application. The bike sharing system securely receives the user's request and communicates securely with the source and destination bike stations to reserve a bike for the user. In the second algorithm, we show how bike distribution management can be done in a secure way so that the system can distribute bikes to various stations according to the real-time demand. The dynamic nature of the distribution system allows it to handle both immediate and future journey demands of the users.

Considering the security issues in the BSS discussed previously and the potential of IoT in BSSs, this paper:

- summarizes a set of services and security requirements for a bike sharing system
- proposes a secure bike sharing and distribution system that has both operator-driven and user-driven functionalities supporting demand-driven reservations for immediate and future journey. Informally, the system provides security as follows:
  - Unless an attacker obtains user's private key or system-wide shared key, no one can impersonate a valid user or a component of the system name, respectively. An attacker cannot obtain the keys as it cannot break the underlying encryption scheme.
  - An attacker cannot falsify a valid information (e.g., bike or parking reservation request, reservation confirmation, external information on weather, event, traffic, etc.) as it is unable to obtain the digital signature key pairs of the system components. Thus the integrity of the information and authenticity of the valid system components are achieved.
  - Since the descriptions of a reserved bike or parking are sent to the user in encrypted form, an attacker cannot link a user's id to a particular bike or parking reservation information. Thus confirming data confidentiality.
- provides security analysis and comparison, in terms of features, with the existing bike sharing systems in the literature.

II. Previous Work

The imbalanced distribution of bikes is a recurrent problem for BSSOs. Rebalancing or redistribution of bikes requires significant logistic work and poses major operational costs to operators. A solution to this problem should know the optimal time, the number of bikes should be removed or placed in each station (e.g., inventory decision) and the way (e.g., cost-effective distribution truck routing) to balance the system. Many solutions have been proposed and these solutions can be divided into two categories: user-driven [1], [5], [6], [7] and operator-driven [8], [9], [10], [11]. In a user-driven approach, the users are incentivized to balance BSSs, whereas in an operator-driven approach, the redistribution is done by the service staffs. Effective utilization of crowdsourcing [1] make user-driven distribution feasible for mid-term operations, but it is highly unpredictable and unsuitable for guaranteed services, especially for short-term users (e.g., work commuters). On the other hand, most operator-driven solutions (e.g., mathematical programming techniques based [11], [12], data mining-based [13], [14]) rely on historical data to find the optimal time, number of bikes to be removed or placed in each station and the way to redistribute the bikes. Real-time information about bikes and bike users, traffic mobility, demand and other factors (e.g., weather, city events) in rebalancing the system are not considered in most of these solutions. This is a critical issue when offering a guaranteed service to the short-term users, especially if bike sharing is integrated with a multi-modal journey plan. A parking reservation policy could improve service quality by guaranteeing a parking space at a destination bike station. Demand estimation, prediction, and service level computation methods for optimal management of bike sharing services has been considered in [15]. However, none of these proposals provides a framework for secure system that allows for integrating bike sharing system into multi-modal journey environment.

III. IoT-integrated BSS

A. Overview of BSS

The main characteristics of next generation BSSs are: (i) increased system flexibility (e.g., demand-responsive) (ii) improved bike distribution, (iii) integration with other transportation modes, (iv) smart bikes. Next generation BSSs with these characteristics should offer the following services:

Reservation Service (RS): This service should allow users to reserve and pay from online using their portable devices or computers. Most existing BSSOs do not support online reservation, they only support designated kiosks-based bike rental services. A reservation request can be made by a rider or by a journey planner (if it is a part of a multi-modal journey plan).

Multi-modal Connectivity (MC): This service will connect a BSS with the multi-modal mobility service chain (e.g., train, bus). It is one of the key requirements of next generation BSSs.

Bike and Parking Availability Check (BPAC): BSSOs need to know (in real-time) the number of available bikes and parking spots in every bike station or list of bike stations before accepting users' reservation requests. Once the availability is confirmed at the requester's preferred station, BSSO confirms the reservation request. In case of bike or parking unavailability in a preferred station, BSSO can check with the bike distribution schedule. If distribution happens sufficiently before the requested start time, BSSO may continue with the reservation request. Otherwise, BSSO will offer the requester with few nearest stations to pick from and if she is happy with one of the alternatives, reservation request is confirmed. In most existing BSSs, users can check the station-wise realtime bike availability before renting one, but cannot pre-book a bike or a parking space.

Bike Distribution Service (BDS): An empty or an overfilled station damages not only the goodwill of a BSSO, but also the business directly in terms of money. BDS continuously monitors users' dynamic demand and refine the system accordingly to meet the demands. This service is the heart of a BSS to maintain service quality and satisfy users. In a BSS, this service can be either operator-driven (ODS) or user-driven (UDS). This service will play a key role in integrating BSSs with other transport modes, especially in journey planning.

B. IoT in BSS

BSSs integrated with IoT will be able to gather enormous amount and variety of data generated by the bike users, bikes and environment. These data can be used to improve existing service quality (e.g., improved BDS, bikers' safety). Most existing BSSs are not IoT-integrated and do not offer all the services summarized in the above section. Few initiatives are underway to integrate bikes as a part of an IoT. Number of BSSs or bike vendors are making smart bikes (e.g., GPS tracker, wireless connectivity) to use dumb docking station and/or kiosk free BSSs.

IV. Preliminaries

In this Section, we explain the notations, system components, setup assumptions, the security properties that we achieve, and a management framework of our proposed system.

A. System Components and Model

A Bike Sharing System (BSS) has the following components: Bike & Parking Availability Check (BPAC), Multimodal Connectivity (MC), Reservation System (RS) and Bike Distribution System (BDS). BDS has the following components: Service Level Manager (SLM), Operator-driven Distribution System (ODS), User-driven Distribution System (UDS) and Inventory Decision Manager (IDM). Different components can communicate with Source Bike Station (SBS), Destination Bike Station (DBS), External Service Providers and Bike Distribution Unit. MC is responsible for communicating with user. External services include traffic, event, location and sensing information collected through Internet of Things (IoT) devices, data analytics services through cloud, etc.

There are S stations in a BSS, C_i is the parking capacity of the station i, B_T is the total number of bikes running in the BSS, P_T is the total number of available parking spaces in the BSS such that $\sum_{i=1}^{S} C_i = B_T + P_T$. The source and destination stations for a bike user are SBS and DBS and the duration of an estimated ride (bike use time) can be estimated using distance between the SBS and DBS or the user provided information during renting or reservation. For the periodic monitoring and operation of a BDS, each day is sliced into 24 time slices as in [16]. The calculations (e.g., demand, reservation threshold) are time slice-specific.

We assume that the BSS management framework has several components. Sensing component consists of sensors and smartphones that are useful for participatory sensing and crowdsourcing. Data management component handles data management, data analysis and demand estimation by integrating heterogeneous sensing, computing and communications devices. The external services layer includes the necessary external services (e.g., weather, location, city events) for different BSSs services.

As discussed earlier, secure multi-modal connectivity and bike distribution schemes are yet to be considered in the BSS level. Section V-B demonstrates the potential of the framework by using it for the proposed BDS.

B. Notations

Table I explains the notations used in this paper.

C. Assumption

It is assumed that BSS is a centralized system where internal components work as different functionalities and the communication between the functionalities is secure. Communication channels between user and BSS, BSS and external service providers, BSS and Bike Distribution Unit, and BSS and Bike Stations are not assumed to be secure. A user registers himself with the system with her ID uid and a shared secret key ku generated by a symmetric key encryption scheme (KCipher-2 [17], for example) through a multi-modal journey planner (MJ), which could be typically a smartphone application software. We assume that MJ can securely collect information on other mode of transportation (e.g., bus or train) from publicly available sources and combine it with bike/parking reservation information to suggest journey options to a multi-modal journey user. MC, BPAC, SLM, SBS, DBS have their digital signature generation and verification key pairs generated by an efficient and secure signature scheme (Schnorr's signature scheme [18], for example. [1]). Components of BSS share a symmetric key k with the stations, external service providers and distribution

[1] Any high-performance symmetric cipher and signature scheme suitable for embedded systems can be used instead of KCipher-2 or Schnorr signature

Table I
NOTATIONS USED IN THIS PAPER

uid	User ID
J_T	Journey Type
k	Shared Secret Key Among BSS, Stations and Other Service Providers
B_a	Total number of bikes available
B_{Res}	Request for Bike Reservation
P_{rn}	Parking Reservation Needed
P_a	No. of available parking
R_p	No. of reserved parking
R_b	No. of reserved bike
R_{pmax}	Maximum allowable R_p
B_{det}	Bike details
P_{det}	Parking details
ku	user's secret key shared with BSS
B_{au}, P_{au}, R_{pu}	Updated B_a, P_a, R_p
P_{NA}	Parking not available
B_{NA}	Bike not available
D_r, D_e	reservation demand, estimated demand
I_{in}, I_c	initial inventory, current inventory,
S_L	service level of a station
S_{Lt}	target S_L of a day,
S_{Lp}	S_L of previous day
S_{Ld}	allowable service level difference
J_d, U_t	journey destination, bike use time
W_{UDS}	willingness to participate in UDS
sk, vk	signing and verification keys of MC
xs, xv	signing and verification keys of external information provider
as, av	signing and verification keys of BPAC
ss, sv	signing and verification keys of SLM
sg, vg	signing and verification keys of SBS
sr, vr	signing and verification keys of DBS
TB_{inc}	total no. of bikes with incentive
Enc_k	Encryption with key k (Enc_{ku} for key ku)
Dec_k	Decryption with key k (Dec_{ku} for key ku)
$Sign_{(\cdot)}$	Signature with signing key $(\cdot)$
$Ver_{(\cdot)}$	Signature verification with key $(\cdot)$

unit. We also assume that BSS, stations, external service providers and distribution units are honest. [2]

Security Properties: Following the discussion in Section I, we briefly describe the security properties in the context of bike sharing system for multi-modal journey below.

- No Impersonation: No entity shall participate in the system with the identity of another entity.
- Unforgeability: No one should be able to falsify a valid information.
- Confidentiality: Attackers should not be able to link a bike and parking details to a particular user.
- Authenticity and Integrity: Authenticity and integrity of all data exchanged between the entities must be verifiable.

D. Reservation Policy

To integrate a BSS into a multi-modal transport systems, a reservation policy for bikes and parking spaces is necessary. This work considers a station-wise (e.g., stations close to train stations or bus stops) short-term reservation policy that allows a fraction of a station's capacity C_i for reservation. It is divided into R_b and R_p for bike and parking spaces. R_{pmax} and R_{bmax} are dynamic values that may change due to peak-hour demand. This can be estimated using the historical reservation demands data. The relationship $R_p + R_b < C_i$ should be true always for a station.

V. PROPOSED SECURE SYSTEM

A. Secure Multi-modal Connectivity Service

The algorithm 1 presents an implementation of the multi-modal connectivity (MC) service using the proposed framework. The algorithm consists of three phases: (i) service availability check, (ii) reservation for an immediate journey and (iii) reservation for a future journey. The implementation uses BDS, BPAC and RS, and these services use components of the framework to maintain multi-modal connectivity. First, we briefly introduce the algorithm and then we move on to explain it formally.

Phase 1: This phase checks service availability. If a BSS service is available, MC receives a reservation request for a specific journey type from a user through MJ. Based on the journey type, phase 2 or phase 3 is activated.

Phase 2: This phase is active when the reservation request is for immediate journey. Upon forwarding the request to BPAC, MC receives the encrypted bike availability information from SBS. BPAC then sends an encrypted bike reservation request and and a signature of the ciphertext to SBS. If the SBS can successfully verify the signature. It then decrypts the ciphertext to check the reservation request, reserves a bike and sends the encrypted details of the reserved bike to RS. If a parking is requested, then DBS sends encrypted parking availability information to RS. RS then encrypts the bike and parking details and sends them to the user. If no parking is available, only reserved bike information is sent to the user. RS updates the number of available bike, parking and reserved parking, andsends them to SBS and DBS in encrypted form.

Phase 3: When a user wants to reserve a bike for future journey then this phase is activated. This phase is almost similar to phase 2, except that the BDS checks the number of reserved bikes at SBS so that it does not go beyond a predefined threshold value). Also, a user may receive an encrypted "bike availability not guaranteed" message (during rush hours or city events when immediate journey reservation gets more priority due to excessive demand, for example).

B. Secure Bike Distribution Service

The proposed BDS is different than the existing operator-driven, user-driven and parking reservation-based BDS as it uses operator-driven and user-driven approaches and supports station-wise demand-driven reservation of bikes and parking spaces. Importantly, it exploits real-time (e.g., users' mobility, bike speed) and non-real-time (e.g., willingness to participate in a UDS W_{UDS}) information about bike users, bikes and environment through IoT-integrated bikes and mobile sensing to improve existing historical data-based demand estimation. Utilizing W_{UDS}

[2] We do not consider key management issues like key revocation, renewal and user revocation in this work.

Algorithm 1 Algorithm for Secure Multi-modal Connectivity

```
User sends a multi-modal journey plan request to the MJ
Phase 1- Service Availability Check
if BSS = $true$ then
    MJ encrypts reservation request $req$ and $J_T$ s.t. $C_0 = Enc_{ku}(req \| J_T)$ and sends $C_0, uid$ to MC via BSS
    MC decrypts $C_0$ using $ku$ of $uid$ and checks $req, J_T$
    if $J_T = 1$ then                                              ▷ for immediate journey $J_T = 1$
        Go to Phase 2
    else Go to Phase 3
    end if
else BSS is unavailable
end if
Phase 2- Reservation for Immediate Journey
MC receives $C_1 = Enc_k(B_a)$ from SBS using BPAC and computes $B_a = Dec_k(C_1)$
if $B_a > 0$ then
    Send $\{C_2 = Enc_k(B_{Res}), \sigma_1 = Sign_{sk}(C_2)\}$ to SBS for reserving a bike
    if $Ver_{vk}(\sigma_1) == 1$ then
        $B_{Res} = Dec_k(C_2)$, a bike is reserved, send $C_3 = Enc_k(B_{det}), \sigma_2 = Sign_{sg}(C_2)$ to RS
        RS verifies $\sigma_2$ using $vg$ and decrypts $C_3$ to get $B_{det}$
        if $P_{rn} = true$ then                                    ▷ if parking is requested
            RS receives $\{C_4 = Enc_k(P_a \| P_{det}), C_5 = Enc_k(R_p), \sigma_3 = Sign_{sr}(C_4 \| C_5)\}$ from DBS
            RS verifies $\sigma_3$ using $vr$ and decrypts $C_4, C_5$ to get $P_a, P_{det}, R_p$
            if  $P_a > 0$ and $R_p \leq R_{pmax}$ then             ▷ if parking is available
                Send $C_6 = Enc_{ku}(B_{det} \| P_{det})$ to user  ▷ confirmed $P_{det}, B_{det}$ are sent to user
                Send $C_7 = Enc_k(B_{au})$, $C_8 = Enc_k(P_{au})$, $C_9 = Enc_k(R_{pu})$ to SBS and DBS
                SBS and DBS decrypt $C_7, C_8, C_9$ to get updated information
            else No parking available                              ▷ $P_{NA}$ = No parking available
            end if
        else Send $C_6 = Enc_{ku}(B_{det} \| P_{NA})$ to user      ▷ confirmed bike details sent to user
            SBS receives $C_7 = Enc_k(B_{au})$, $C_8 = Enc_k(P_{au})$ from RS and updates accordingly
        end if
    else Error
    end if
else No bike available at SBS
    Send $C_{12} = Enc_{ku}(B_{NA})$ to user                       ▷ $B_{NA}$ = Bike not available
end if
Phase 3- Reservation for Future Journey
MC receives $C_1 = Enc_k(B_a)$ from SBS and computes $B_a = Dec_k(C_1)$
if $B_a > 0$ then
    Send $\{C_2 = Enc_k(B_{Res}), \sigma_1 = Sign_{sk}(C_2)\}$ to SBS for reserving a bike
    if $Ver_{vk}(\sigma_1) == 1$ then
        $B_{Res} = Dec_k(C_2)$
        BDS receives $\{C_{10} = Enc_k(R_b), \sigma_4 = Sign_{sg}(C_{10})\}$ from SBS, verifies $\sigma_4$, computes $R_b = Dec_k(C_{10})$
        if  $R_b \leq R_{bmax}$ then                               ▷ bike reservation allowed
            Reserve a bike and parking at the SBS and DBS as in Phase 2
        else Bike availability is not guaranteed
            Send $C_{11} = Enc_{ku}(B_{NG})$ to user               ▷ $B_{NG}$ = Bike availability not guaranteed
        end if
    else Error
    end if
else No bike available
    Send $C_{12} = Enc_{ku}(B_{NA})$ to user                       ▷ $B_{NA}$ = Bike not available
end if
```

information received from users during renting or reservation in the BDS's incentive offer will motivate more users to participate in UDS. For instance, if a user gets an incentive offer (e.g., free 10 minutes) for a future distribution at the time of renting or reservation, she can manage her time better than if she gets the offer at the time of a bike return. ODS and UDS approaches are complementary to each other. The former one works mainly to handle the imbalances at a macro level by moving the bikes from a part of the city to the other, and the later one is dynamic and generally works at a micro level, incorporating the traffic flow and fluctuating demands. The BDS incorporates reservation policy to improve service quality, especially for short-term and BSS-integrated multi-modal transport users. A bike user in a multi-modal journey could miss her next mode of transport (e.g., train or bus) because of an empty or a full bike station. Initial distribution is static and generally operates during the night time when the congestion and demands are low.

A key factor to the success of a BSS is its reliable handling capability of its dynamic demands. To cope with dynamic demands, the BDS aims to improve the dynamic demand estimation method [15], using high resolution and real-time, and non-real-time information about the bike users, reservation demands, application environments (e.g., stations road condition), weather, city events, etc. The inventory, optimal time and route decision mechanisms are briefly mentioned in the following.

Bike users' type (e.g., registered, casual, short-term), which directly influences bikers' behavior model, can play an important role in type-wise bike demand estimation, BDS (e.g., user-driven distribution) implementation and improving service quality (e.g., offering reservation for short-term users). Bike users can be registered (i.e., yearly or monthly) or causal (e.g., tourists), which also can be short-term users (e.g., 30-45 minutes) or medium-term users (e.g., more than 30-45 minutes). If D_e is the estimated bike demand for a station, it can be expressed as a linear combination of the estimated non-reservation demand D_{enr} and estimated reservation demand D_{pr} as: $D_e = \alpha D_{enr} + \beta D_{er}$, where α and β are demand sharing factors such that $\alpha + \beta = 1$. Likewise, we can estimate parking demand Dp_e for a station. D_e and Dp_e represent target inventory of a station for a specific time period such that $D_e + Dp_e \leq C$. In a system, user-driven BDS DS_u and operator-driven BDS DS_o complements each other, where DS_u and DS_o are functions of D_e and Dp_e. Especially, DS_u is a function that takes as input estimated non-reserved bike and parking demands (D_{enr}, Dp_{enr}) and outputs the current demand estimation of a particular time slot during a BDS, where $DS_u = Dp_{enr} - D_{enr}$.

Once the target inventory information (D_e, DP_e) are available, it is important to estimate whether near future's UDS will be able to maintain the target inventory or not. If not, an ODS should be operated based on service level (service level = (number potential of customers - number of unsatisfied customers)/ number of potential customers; where the " number of unsatisfied customers" corresponds to the customers who could not rent a bike at an empty station or failed to return their bike at a full station.), which is continuously computed using users feedback. If the service level drops below a pre-determined threshold value, ODS is operated. An optimal routing mechanism of a distributor truck our algorithm utilizes the method described in [7]. Algorithm 2 describes the BDS framework formally.

VI. Security Analysis and Evaluation

A. Security

- *No Impersonation:* Unless an attacker obtains user's private key ku or system-wide shared key k, no one can participate in the system in user's name or in system's name, respectively. Also, the key k is assumed to be securely stored with the BSS and other entities. So, the attacker can not break into them. If an attacker seeks to determine the keys from the public information, then he must use one of the following methods:
  1) The attacker derives ku: this requires breaking the security of underlying symmetric key encryption scheme. Note that, ku is available to BSS and the user only.
  2) The attacker gets k from the communication channel between BSS and other entities (i.e., stations, distribution unit and external service providers). In order to do so, he needs to break the security of underlying symmetric key encryption scheme.
- *Unforgeability:* An attacker cannot obtain $\{sk, vk\}, \{xs, xv\}, \{as, av\}$, $\{ss, sv\}$, $\{sg, vg\}$ and $\{sr, vr\}$ key pairs to forge MC, external service providers, BPAC, SLM, srouce station and destination station, respectively. The attacker needs to break the unforgeability property of the underlying signature scheme. This analysis confirms that an attacker cannot generate a valid message-signature pair where the message has not been signed by the legitimate signer.
- *Confidentiality:* Since the descriptions of a reserved bike or parking is encrypted and sent to the user, an attacker cannot link a user id to a particular bike or parking reservation information. The attackers will have to break the security of underlying encryption scheme to be able to link a biker's id and her reserved bike/parking information.
- *Authentication and Integrity:*
  1) Request req: Authenticity and integrity of the requests req sent by the MC, BPAC and SLM are preserved due to the use of Schnorr signature scheme. No other entity other than the MC, BPAC and SLM can generate a valid signature while sending req to the stations. Also, req cannot be modified by an adversary since the integrity of req is verifiable through the signature.

Algorithm 2 Algorithm for Secure Bike Distribution System

```
Phase 1- Static Inventory
For each station $i$, IDM gets $\{C_1 = Enc_k(D_r), C_2 = Enc_k(I_{in})\}$ from $i$ through MC or RS and computes $\{D_r = Dec_k(C_1), I_{in} = Dec_k(C_2)\}$
IDM estimates demand $D_e$
IDM gets $S_{Lt}$, $S_{Ld}$ $S_{Lp}$ from SLM
if $S_{Lt} - S_{Lp} > S_{Ld}$ then    ▷ $S_{Lt} = \lfloor|$avg. $S_L$ on that day $+$(current $S_L - S_{Lp}$)$|\rfloor$
    Computes distribution request ($D_{dr} = |I_{in} - I_c|$) and sends to ODS
    ODS computes $C_3 = Enc_k(D_{dr})$ and sends to distribution unit
    Distribution Unit decrypts $C_3$ using shared key $k$ to get $D_{dr}$, and sends bikes accordingly
end if
Phase 2- User Driven System
for each time slot do
    UDS and IDM get $\sigma = Sign_{xs}$(external information)
    UDS and IDM Verify $\sigma$ using $xv$
    for each station $i$ do
        BPAC and SLM send signed requests $\{req, \sigma_1 = Sign_{as}(req)\}$ and $\{req, \sigma_2 = Sign_{ss}(req)\}$ to $i$
        station $i$ verifies $\sigma_1$ and $\sigma_2$ using $av$ and $sv$, respectively
        station $i$ sends $C_4 = Enc_k(I_c)$ and $C_5 = Enc_k(S_L)$ to BPAC and SLM, respectively
        BPAC and SLM decrypt $C_4$ and $C_5$ to get $I_c$ and $S_L$, and forward them to UDS
        UDS receives $C_6 = Enc_k(J_d \| U_t \| W_{UDS})$ from $i$, decrypts them, and computes $DS_u$
        IDM estimates bike and parking demand $D_e$ for next time slot and sends it to UDS
        SLM receives external information from UDS, and computes $S_{Lt}$ from them
        SLM shares $S_{Lt}$, $S_{Ld}$ with UDS
        while $TB_{inc} \leq B_{max}$ do    ▷ $B_{max}$ = maximum no. of bike
            if $S_{Lt} - S_L > S_{Ld}$ and $D_e > I_c + DS_u$ then
                Offers encrypted incentive to $W_{UDS}$ users $C_7 = Enc_{ku}(inc)$ via MC
                if not sufficient response from users then
                    UDS offers other users to participate
                end if
            end if
            Update $DS_u$
        end while
        $S_c = S_c + 1$    ▷ $S_c$ = Stations performing critically
    end for
    go to Phase 3
end for
Phase 3- Dynamic Operator Driven System
ODS gets the $DS_u$ of critical stations from UDS
if $S_c > S_{cth}$ then    ▷ $S_{cth}$ = number of critically performing stations allowed before ODS
    ODS computes $C_3 = Enc_k(D_{dr})$ and sends $C_3$ to distribution unit    ▷ $D_{dr} = D_e - I_c - DS_u$
    Distribution Unit decrypts $C_3$ using shared key $k$ to get $D_{dr}$, and sends bikes accordingly
end if
Go to phase 2
```

2) User Authentication: A user is authenticated by the system by her uid. The system has stores uid and the corresponding key ku in its database. When a user sends encrypted req, J_T (under her key ku) to the system, the system looks up its database using uid and authenticates the user if it can decrypt the received ciphertext. As an attacker cannot get ku, he cannot authenticate himself wth the system.
3) Service information: Authenticity and integrity of the external information of each information service providers are also achieved. Each service provider signs its information before sending them to UDS and IDM. In order to break the authenticity and integrity, an attacker needs to break the unforgeability of the underlying signature scheme.

B. Evaluation

Table II summarizes a comparative evaluation between our proposed system and existing BDS schemes in terms of type, integration of multi-modal journey, reservation options, types of information used, authenticity, integrity, unforgeability, no impersonation, and confidentiality. It shows that our proposed system has the potential to perform better both in terms of security and features in next-generation BSSs compared to most existing BDS.

Table II
COMPARISON WITH RELATED WORK

	This Work	[1]	[12]	[16]
Type	ODS, UDS	UDS	ODS	ODS, UDS
Reservation Support	Bike, Parking	No	Parking	Bike, Parking
Information Source	real-time, historical	historical	historical	real-time, historical
Multi-modal Journey Support	Yes	No	No	Yes
Authenticity	Yes	No	No	No
Integrity	Yes	No	No	No
Unforgeability	Yes	No	No	No
No Impersonation	Yes	No	No	No
Confidentiality	Yes	No	No	No

VII. CONCLUSIONS

This paper proposes a framework for secure bike sharing service under multi-modal journey environment using symmetric key encryption and digital signature. Through this framework, a service operator can collect relevant information from stations and external service providers, and can communicate with users in a secure way to provide correct information to a user. The framework allows to maintain a flow of correct data throughout the system so that the service is not disrupted. The proposal, using IoT-provided real-time and non-real-time information, has the potential to offer better service quality compared to most existing BDS, especially to BSS-integrated multi-modal transport users in smart cities.

REFERENCES

[1] A. Singla, M. Santoni, G. Bartók, P. Mukerji, M. Meenen, and A. Krause, "Incentivizing users for balancing bike sharing systems," in *Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence, January 25-30, 2015, Austin, Texas, USA.*, 2015, pp. 723–729.

[2] A. Spickermann, V. Grienitz, and H. A. von der Gracht, "Heading towards a multimodal city of the future?: Multi-stakeholder scenarios for urban mobility," *Technological Forecasting and Social Change*, vol. 89, pp. 201 – 221, 2014.

[3] G. Kortuem, F. Kawsar, V. Sundramoorthy, and D. Fitton, "Smart objects as building blocks for the internet of things," *IEEE Internet Computing*, vol. 14, no. 1, pp. 44–51, 2010.

[4] Bayless, Murphy, and Shaw, "Cybersecurity and dependable transportation: System assurance, operations and reactive defense for next generation vehicles and intelligent highway infrastructure," 2012.

[5] D. Chemla, F. Meunier, T. Pradeau, R. Wolfler Calvo, and H. Yahiaoui, "Self-service bike sharing systems: simulation, repositioning, pricing."

[6] M. Rainer-Harbach, P. Papazek, B. Hu, and G. R. Raidl, "Balancing bicycle sharing systems: A variable neighborhood search approach," in *Evolutionary Computation in Combinatorial Optimization: 13th European Conference, EvoCOP 2013, Vienna, Austria, April 3-5, 2013. Proceedings*, 2013, pp. 121–132.

[7] J. Pfrommer, J. Warrington, G. Schildbach, and M. Morari, "Dynamic vehicle redistribution and online price incentives in shared mobility systems," *Intelligent Transportation Systems, IEEE Transactions on*, vol. 15, no. 4, pp. 1567–1578, Aug 2014.

[8] L. Caggiani and M. Ottomanelli, "A modular soft computing based method for vehicles repositioning in bike-sharing systems," *Procedia - Social and Behavioral Sciences*, vol. 54, pp. 675 – 684, 2012, proceedings of {EWGT2012} - 15th Meeting of the {EURO} Working Group on Transportation, September 2012, Paris.

[9] ——, "A dynamic simulation based model for optimal fleet repositioning in bike-sharing systems," *Procedia-Social and Behavioral Sciences*, vol. 87, pp. 203–210, 2013.

[10] D. Chemla, F. Meunier, and R. W. Calvo, "Bike sharing systems: Solving the static rebalancing problem," *Discrete Optimization*, vol. 10, no. 2, pp. 120 – 146, 2013.

[11] J.-R. Lin, T.-H. Yang, and Y.-C. Chang, "A hub location inventory model for bicycle sharing system design: Formulation and solution," *Comput. Ind. Eng.*, vol. 65, no. 1, pp. 77–86, May 2013.

[12] T. Raviv, M. Tzur, and I. A. Forma, "Static repositioning in a bike-sharing system: models and solution approaches," *EURO Journal on Transportation and Logistics*, vol. 2, no. 3, pp. 187–229, 2013.

[13] J. Froehlich, J. Neumann, and N. Oliver, "Sensing and predicting the pulse of the city through shared bicycling," in *Proceedings of the 21st International Jont Conference on Artifical Intelligence*, ser. IJCAI'09, Pasadena, California, USA, 2009, pp. 1420–1426.

[14] A. Kaltenbrunner, R. Meza, J. Grivolla, J. Codina, and R. Banchs, "Urban cycles and mobility patterns: Exploring and predicting trends in a bicycle-based public transport system," *Pervasive Mob. Comput.*, vol. 6, no. 4, pp. 455–466, Aug. 2010.

[15] P. Borgnat, P. Abry, P. Flandrin, C. Robardet, J.-B. Rouquier, and E. Fleury, "Shared bicycles in a city: A signal processing and data analysis perspective," *Advances in Complex Systems*, vol. 14, no. 03, pp. 415–438, 2011.

[16] M. Razzaque and S. Clarke, "Smart management of next generation bike sharing systems using internet of things," in *Smart Cities Conference (ISC2), 2015 IEEE First International*, Oct 2015, pp. 1–8.

[17] S. Kiyomoto, T. Tanaka, and K. Sakurai, "K2: A stream cipher algorithm using dynamic feedback control," in *SECRYPT 2007, Proceedings of the International Conference on Security and Cryptography, Barcelona, Spain, July 28-13, 2007*, 2007, pp. 204–213.

[18] C. Schnorr, "Efficient identification and signatures for smart cards," in *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, 1989, pp. 239–252.