Research Article

A Luggage Control System Based on NFC and Homomorphic Cryptography

Néstor Álvarez-Díaz,¹ Pino Caballero-Gil,¹ and Mike Burmester²

¹Department of Computer Engineering and Systems, University of La Laguna, Tenerife, Spain

²Department of Computer Science, Florida State University, Tallahassee, FL, USA

Correspondence should be addressed to Néstor Álvarez-Díaz; nalvared@ull.edu.es

Received 15 September 2016; Revised 17 December 2016; Accepted 12 January 2017; Published 15 February 2017

Academic Editor: Alessandro Bazzi

Copyright © 2017 Néstor Álvarez-Díaz et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

We propose an innovative luggage tracking and management system that can be used to secure airport terminal services and reduce the waiting time of passengers during check-in. This addresses an urgent need to streamline and optimize passenger flows at airport terminals and lowers the risk of terrorist threats. The system employs Near Field Communication (NFC) technology and homomorphic cryptography (the Paillier cryptosystem) to protect wireless communication and stored data. A security analysis and a performance test show the usability and applicability of the proposed system.

1. Introduction

Air transport is currently in a period of rapid expansion. For sustainable growth a number of issues need to be urgently addressed. In particular, it is essential to efficiently manage luggage and passengers and guarantee the secure operation of the services provided at airport terminals. The optimization of passenger flows at airport terminals is currently an emerging research topic, with the most innovative proposals addressing the efficiency and security of the check-in procedure, baggage drop-off, and seat assignments. Our contribution in this work is to propose a novel luggage management system that optimizes and secures this process.

There are several reports on passenger expectations and satisfaction of the services provided at airport terminals (see, e.g., [1]). These highlight a number of issues that need to be addressed. For example, issues related to luggage [2], such as luggage management, real-time luggage control, and autolabelling of luggage, have been suggested as points that reflect a general dissatisfaction among passengers. The most common reason for complaints is the tightening of controls following recent terrorist attacks and the security checks to prevent such attacks (security checking often produces long

waiting lines). To address such issues our proposal describes a mechanism that lets airport users manage their luggage, focusing on increased control, and provides the possibility of real-time luggage monitoring.

There has been a great change in passenger attitude towards using new technologies at airports (see, e.g., [3]), in particular, wireless technologies such as Radio Frequency Identification (RFID), typically used for inventory management, and Near Field Communication (NFC). Their ability for automatic identification and their flexibility for contactless data transfer make them ideally suited for air transport management applications.

RFID was adapted from supply chain logistics to the air transport sector by British Airways in 1999 for baggage tagging, to replace barcode tagging. In 2005, the International Air Transport Association (IATA) released the Recommended Practice RPI740C Report [4] that defined the use of RFID tags and readers for baggage tags. The benefits of RFID were extensively investigated by IATA that predicted an expected increase in the security of baggage handling by better tracking of screened baggage. However RFID baggage tagging has not been yet implemented on a wide scale. It remains an isolated application without an integrated implementation among various infrastructures or

services, mainly due to the difficulties in reaching a global agreement.

Regarding the use of NFC technology for air transport, several airlines have piloted the introduction of NFC for the transmittal of boarding card data and frequent traveller authorization. In 2009, NFC was tested for the transmittal of boarding cards in the “Pass-and-Fly” trial by Air France. A few years later, Suparta [5] proposed the adoption of NFC technology to enhance ticketing systems with mobile platforms at airports for more efficient ticketing, gating, and aircraft boarding. That work does not address security issues or baggage tracking. Curran et al. [6] have analysed the possibilities for security relevant applications and their implications and impact for passengers. Our proposal can be seen as a practical approach for securing airport passenger management operations using NFC technologies. We note that the application of NFC technologies for aviation security matters has not yet been addressed.

According to industry surveys, smartphone use for air travel services is increasing. Approximately 80% of passengers use self-service automation and 72% carry a smartphone. Thus, once the use of NFC enabled smartphones approaches saturation, it will become possible to use this technology for the benefit of passengers in general.

The main objective of our proposal is to provide a system for permanent luggage labelling through NFC tags for identifying the owner of luggage as well as tracking luggage throughout the airport, taking into account security requirements, including privacy, authentication, and data integrity. Regarding related proposals, as mentioned earlier, the British Airways system [7] uses permanent labelling, with the label automatically configured and printed in an electronic ink label, and employs RFID technologies (mainly NFC) [8]. However, the objective of this system is luggage tracking, not security, which is the objective of the present proposal.

In the proposed system, the current state of luggage is known at all times by the airport authorities thanks to the use of NFC readers and tags. Since current smartphones are starting to adopt this technology, passengers will also be able to check their luggage through a mobile phone application. Those passengers, who do not have access to NFC technology, will be offered the possibility of accessing a check-in desk equipped with NFC technology at the airport. Thus, as with the current availability of online check-in, passengers will be offered a faster luggage check-in procedure.

This document is structured as follows. Section 2 introduces the objectives and requirements of our luggage control system. Section 3 briefly mentions some key aspects of the main components of the system. Section 4 describes the complete structure of the system, paying special attention to the internal operations related to data flows. The cryptographic tools that provide reliability for luggage control, as well the authentication and confidentiality protection, are described in Section 5. Several possible vulnerabilities and attacks to the system are analysed in Section 6. A brief performance analysis of cryptographic tools and the NFC technology is included in Section 7. We conclude in Section 8 with some open problems.

2. Overview of the Proposal

The proposed luggage control system has two objectives that are tightly linked: the optimization of luggage check-in and the increase of airport security through a higher baggage control [9]. To achieve these objectives it identifies the passengers and their luggage and tracks the luggage from the time it is delivered (bag drop) to the time it is collected (baggage claim).

A diagram of the proposed system is shown in Figure 1. This represents the interaction through different types of networks among the different elements that compose the system. First, it shows the actions of passengers regarding their luggage: Registration, Online Check-In, and Baggage Delivery (bag drop). Each one of these actions will be explained in detail below. Second, the diagram describes the process between the airport server and the certification authority for updating keys through a secure communication channel. Note that the airport server is responsible for registering new luggage and generating the boarding pass and the set of data for the luggage NFC tags. The communication between the airport server and each control point allows updating the luggage status. Finally, the part indicated in the diagram as “Control and Management” includes the cycle that each bag undergoes from the Delivery Point to the bag claim through each control point. A detailed overview of the complete process is described below.

- (A) *Registration (Figure 2)—The First Time.* The passenger registers at the airport. Airport agents identify the passenger and update the passenger’s records in the system and provide the passenger with the required NFC tags: one tag for each bag. Then, the passenger can attach an NFC tag to each bag permanently, so that a new tag will not be required for the next flight. After this first step, the system will know the identity of every passenger who is linked to an NFC luggage tag.
- (B) *Online Check-In (Figure 3(B)).* On the same web platform or mobile applications used for online check-in, the passenger can register their luggage for a flight. After registering the luggage, the system returns the encrypted and signed data corresponding to the flight so that this information can be written automatically to NFC tags.
- (C) *Baggage Delivery Point (Figure 3(C)).* After configuring the NFC tag, the passenger can drop the luggage at the airport baggage Delivery Point, where the identification of the passenger as well as the authenticity and integrity of data stored on the tag are verified.
- (D) *Control of Luggage Management (Figure 3(D)).* Information about the luggage management process is added to the NFC tag at each control point, from the Delivery Point at the original airport to its placement inside the airplane, until the passenger receives its luggage at the baggage claim at the destination airport.

FIGURE 1: General communication diagram for the luggage control system.

FIGURE 2: System process: registration.

3. Components of the System

The luggage control system has several components with different functions:

- (i) *Server, S*, which allows managing passengers and luggage. This is a central element of the system because it grants check-in access to passengers and luggage and registers state changes and tracking data for each bag. Furthermore, the server is endowed with the ability to encrypt and decrypt NFC tag content, being the only entity with these permissions.
- (ii) *Smartphones and airport check-in points*, which are used to write data on NFC tags. When passengers check-in their luggage, the attached NFC tags are written with the configuration data. These system elements can only write to the tags and do not possess the ability to read stored information.
- (iii) *NFC tags*, which allow registering the set of states that luggage has reached. The fact that the tag update operation is available implies a more exhaustive control of the luggage. In current systems and other proposals, updating information stored on baggage tags is not possible due to the fact that the labels used are printed bar codes, so their substitution is impractical.
- (iv) *Control points*, C_v ($v = 1, 2, \dots, P$), which are responsible for verifying that the information stored on NFC tags has not been altered, as well as for updating the current state of the luggage on the NFC tag and the server. Real-time tracking of luggage is therefore possible. For this reason, at each point C_v , there is an NFC reader that allows reading and writing to NFC tags. Moreover, in the most critical points in relation to security, like delivery points, the presence of personnel who can verify the content of the luggage physically through X-rays, for example, would be advisable.

- (v) *Verification authorities*, which are located in some control points and have the function of deciding the normal cycle for each bag and notifying any incorrect state if the situation requires it.

In order to minimize the requirements for the deployment of the system and to enable the gradual integration of airports, the operational independence between airports is a key factor. In the above basic scheme, the unique entity with the ability to decrypt the content of NFC tags is the server S , which provides the user with the corresponding data and boarding pass. However, this restriction could cause a problem rather than a solution if it is necessary to decrypt the content of the tag at the destination airport. To solve this aspect, as shown in Figure 4, between the departure airport and the airplane and between the airplane and the destination airport, the content of NFC tag is changed at each control point, but the original data stored in the tag do not change. In the following proposal the airplane plays the role of intermediary between airports to avoid that each airport has to know the public key of each other airport. With this idea, a distributed model is proposed based on the following concepts:

- (i) *Distributed servers* across different airports, so that each airplane carries the flight keys and both airports' keys.
- (ii) *Flight keys*, which are one-use keys with the sole purpose to act as relay between airports by decrypting/encrypting NFC tags. The process is carried out as follows: firstly, the server of the airplane requests a new pair of public/private flight keys; secondly, it sends to the departure airport the information of the tag together with the obtained public key; thirdly, the airport's server decrypts the content with its private key and encrypts it with the provided public key; finally, the airport's server returns the altered data to the airplane's server. At the destination airport, a similar process is carried out between the destination airport and the airplane.
- (iii) *Certification authority*, which is a central element of the system because its main role is to certify all the keys.

4. Internal Operations

The whole system is represented in the flow chart of Figure 5, where four sections are distinguished and their respective operations are organized.

The section corresponding to the passenger appears two times because it is a flow chart represented as a timeline. The passenger check-in must be always the first operation, independently of whether the airport applies or not the proposed system. After that, the passenger has two options depending on whether his or her luggage has the NFC tag.

If the departure airport has implemented the luggage control system, then the control and verification process shown in the diagram of Figure 5 is applied. The cycle of verification has some critical steps so that if some of them

FIGURE 3: System process: Check-In, Baggage Delivery Point, and Control and Management.

fail, the verification authorities can try to solve the situation by either returning the bag to the original flow or pushing it aside and reporting the safety equipment. In this case, if a bag comes to the safety equipment, it is considered out of the system control. The first part of the cycle concludes when the bag crosses the last control point before the airplane takes off.

The control point of the airplane generates a pair of flight keys certified by the corresponding certification authority. The airplane server sends the public key (KPU) and the content of each NFC tag to the departure airport server in order to receive it back encrypted with the flight key. When the airplane arrives at the destination airport, exactly the

same procedure is carried out. If the process finishes without incidents, the last step is a verification of the passenger who collects the luggage at the destination airport.

Different corrective measures and safety actions could be used at each airport, but to standardize the process, a few bytes of the NFC tag should be dedicated to indicate any possible abnormal situation. Thus, a set of control codes can be devoted to this purpose so that they must be also encrypted, as part of the content of the NFC tag.

If the departure airport has not implemented the luggage control system, then passengers can write an instruction to their mobile application indicating this and deliver their

FIGURE 4: Flight keys and data transmission operations.

luggage using the current procedure. This implies that from the Delivery Point to the airplane, no additional process is carried out by this system.

5. Cryptographic Tools

Since the proposed luggage control system manages sensitive information and since NFC tags can easily be read or written by mobile applications, the protection of privacy, confidentiality, integrity, and authenticity of stored data is essential.

The following procedure is used to protect and update stored information (Figure 6).

(i) Steps $[p(1)-p(3)]$ are executed by passengers after registration.

p(1) Online Check-In, Boarding Pass, and NFC Tag Data. Passengers obtain their boarding pass together with the data to be written to NFC tags through a mobile application. The data is encrypted and digitally signed with the public encryption key and signature key of the airport server S . This step involves transferring data from the airport server to passenger smartphones. Note that the server has two pairs of keys, one for encryption/decryption and the other for digital signatures/verification.

p(2) Write Data to NFC Tags. Passengers write the transferred data to NFC tags using a mobile application.

p(3) Check-In and Baggage Drop-Off. Passengers check in and drop off their baggage at the airport terminal. The first control point C_1 is located at this platform to identify passengers, check the integrity of data written to NFC tags, and verify that the relation between passengers and their baggage is correct.

(ii) Steps $[c(1)-c(4)]$ are executed at each control point C_v after baggage drop-off.

c(1) Read NFC Tags. C_v reads NFC tag data to get their serial number N and the encrypted and signed data. To check the integrity and authenticity of the (encrypted) message, C_v verifies the digital signature of C_{v-1} when $v > 1$ and the server S when $v = 1$. If the verification fails, the baggage is set aside for further checking.

c(2) Homomorphic Cryptography [10]. Homomorphic cryptography is used so that C_v can update data stored on NFC tags without decrypting it. For our luggage control system the server is the only entity that can decrypt data stored on tags. To update encrypted tag data without homomorphic cryptography, this would require interaction between C_v and the server, a burden on system resources and network traffic.

c(3) Write to NFC Tags. C_v updates the (encrypted) message and writes this to the NFC tags together with its digital signature on the updated message.

c(4) Update Database (DB). C_v sends the digitally signed messages of the tags to the server S who verifies their signature and checks the updated messages for correctness. If they are valid, they are stored in DB.

As shown in Figure 7, at each control point, it is necessary to add data to that already stored on a tag to indicate that the baggage has crossed a control point. To identify which point has been crossed, a signature is used. For signature verification, each control point C_v must know the previous point C_{v-1} (or the first one if $v = 1$).

FIGURE 5: Flow chart of the complete system.

FIGURE 6: Data transmission scheme.

FIGURE 7: Data verification and update at each control point.

When the server S decrypts the information stored in a luggage tag, the result must always reflect the number of control points through which that bag has passed.

The Paillier Cryptosystem. The Paillier cryptosystem [11] is a public key scheme based on the problem of computing n th residue classes. It is one of the two most commonly used additive homomorphic cryptosystems (the other one being an extension of the Paillier system with bilinear groups). We briefly describe it below.

Key Generation

- (1) Choose two large prime numbers p and q randomly and independently such that $\gcd(pq, (p-1)(q-1)) = 1$.
- (2) Compute $n = pq$, $\lambda = \text{lcm}(p-1, q-1)$.
- (3) Select a random generator $g \in \mathbb{Z}_{n^2}^*$ and ensure that n divides the order of g by checking the existence of the modular multiplicative inverse: $\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n$, where the function L is defined as $L(u) = (u-1)/n$.

- (4) The public key is $KPU = (n, g)$ and the private key is $KPR = (\lambda, \mu)$.

Encryption. To encrypt the message $M_i \in \mathbb{Z}_n$, select a random number $r \in \mathbb{Z}_n^*$ and compute the ciphertext: $C_i = g^{M_i} \cdot r^n \bmod n^2$.

Decryption. To decrypt the ciphertext $C_i \in \mathbb{Z}_{n^2}^*$, compute the plaintext: $M_i = L(C_i^\lambda \bmod n^2) \cdot \mu \bmod n$.

Digital Signature. To sign the message $M_i \in \mathbb{Z}_n$, compute the digital signature (t_1, t_2) :

$$\begin{aligned} t_1 &= \frac{L(H(M_i)^\lambda \bmod n^2)}{(g^\lambda \bmod n^2)} \bmod n, \\ t_2 &= (H(M_i) \cdot g^{-t_1})^{n^{-1} \bmod \lambda} \bmod n, \end{aligned} \quad (1)$$

where $H() : \{0, 1\}^* \rightarrow \mathbb{Z}_{n^2}^*$ is a cryptographic hash function.

Verification. To verify the signature (t_1, t_2) on message M_i , check whether $H(M_i) \stackrel{?}{=} g^{t_1} \cdot t_2^n \bmod n^2$. If this holds, output is valid. Otherwise output is invalid.

The most interesting property of the Paillier cryptosystem for the present application is its homomorphic property with respect to the addition of plaintexts: given plaintexts $M_1, M_2 \in \mathbb{Z}_n$ and the corresponding ciphertexts $C_1 = E(M_1)$, $C_2 = E(M_2)$, we have

$$\begin{aligned} (C_1 \cdot C_2) \bmod n^2 &= (E(M_1) \cdot E(M_2)) \bmod n^2 \\ &= (g^{M_1} \cdot r_1^n) \cdot (g^{M_2} \cdot r_2^n) \bmod n^2 \quad (2) \\ &= E((M_1 + M_2) \bmod n). \end{aligned}$$

Thus the sum of the plaintexts can be obtained from the product of the corresponding ciphertexts. For our implementation we extend this property to

$$\left(\prod_{i=1}^P E(M_i) \right) \bmod n^2 = E\left(\left(\sum_{i=1}^P M_i \right) \bmod n \right), \quad (3)$$

where P is the total number of control points. For the simplest application we use the property

$$D(E(M) \cdot (g^P \cdot r^n) \bmod n^2) = (M + P) \bmod n, \quad (4)$$

where M is the message whose encryption was stored originally on the NFC tag during check-in and P is the number of crossed control points.

Note that the parameters should be chosen such that $n > (M + P)$, to be able to use the decryption to check the number of control points. Thus, thanks to the additive homomorphic property of the encryption scheme, after crossing the last control point, the server can check that the luggage has gone through all control points.

6. Security Analysis

Several vulnerabilities related to the employed technology and implementation of the luggage control system are discussed below.

Regarding vulnerabilities of the employed technology, two practical issues have been identified that are similar to those of current systems based on printed barcode labels. The first is related to physical protection and concerns baggage that is not properly NFC-tagged. Such baggage will be rejected at the Delivery Point (drop bag). To address this issue in our implementation we propose that the airport security agents apply the most convenient procedure, for example, use the current method based on printed labels. The second issue concerns faulty, corrupted, or unreadable NFC tags. In this case, if the first control point has verified that the information stored on the tag was correct when the passenger handed the luggage at the Delivery Point, then we proceed as in the previous case. Otherwise (e.g., if the tag is unreadable, or a digital signature is not valid), the luggage needs to be checked again by airport agents, registered, and relabelled.

Several attacks can exploit the technology used. A malicious user may try to change the content of an NFC tag. There are many mobile applications that can be used for such an attack. However the digital signature on the stored data will detect compromised data. We note that throughout the luggage tracking process, data stored on NFC tags (including signatures) is updated at each control point. This provides a mechanism for controlling the management of baggage. Airport security agents that manage the luggage control system are assumed to be honest, so they are not supposed to be adversarial. Thus, the protection of the luggage control system is against external threats. Finally, regarding the use of the Paillier cryptosystem, since it is nondeterministic (i.e., the same message is encrypted differently each time), the system is resistant to unauthorized tracking.

In the following sections we analyse attacks that exploit the wireless medium of NFC technologies [12].

6.1. Eavesdropping. Wireless communication is particularly vulnerable to eavesdropping attacks. Though NFC technology is wireless technology, its range is very short (between 6 cm and 10 cm), which makes eavesdropping much harder than with other wireless technologies. Nevertheless, with appropriate receivers, an attacker can intercept the signal. In the proposed system, before baggage delivery, it is impossible to prevent such attacks. After baggage delivery, the secure area of the airport is a zone endowed with access control that offers some protection, but ultimately this type of attack can always succeed. However the cryptographic encryption will not allow the attacker to access the plaintext data on NFC tags.

6.2. Data Modification and Data Insertion. The system provides protection against data modification and data insertion thanks to the use of digital signatures. In particular, the NFC tags used in the beta implementation of the system use 3 KB of the total user space for messages and signatures. If an attacker tries to change or add information to the NFC tag, the system detects several types of anomalies at the moment of verification:

- (i) When a control point tries to verify a signature but cannot separate the message from the signature because the written data are invalid, the bag is separated from the normal flow in order to check the integrity of stored data.
- (ii) If a modification affects only the message part, when checking the integrity of data through the signature, the result will be invalid.
- (iii) When a modification affects only the signature part, as in the previous case, if the control point tries to execute the verification, the result will be invalid.

6.3. Man in the Middle. In a man in the middle attack the adversary interposes between a tag and the reader to intercept and relay messages between both parties and gain access to private information. However this type of attack is practically impossible over NFC links since NFC readers can detect changes of the signal and collisions.

6.4. Tag Cloning. Tag cloning is a simple attack that cannot be detected with cryptographic protection. There are several applications for cloning NFC tags. However, the tags used in the beta implementation of this work have a static field that is used for the verification through the signature. In a real situation, when an attacker clones a tag, he or she can clone all the content except the static field. Thus, the use of a combination of static and dynamic information allows protecting the system against tag cloning. Note that there is a tradeoff between unclonability and untraceability. To make a device unclonable, since cryptographic protection does not help, one has to rely on static information. That can be used to identify a cloned device but can also be used for unauthorized tracking. In the case of NFC tags, for security applications like tracking/managing, unclonability (integrity) is more important than untraceability (privacy). Therefore, the proposal fulfills this unclonability requirement at the cost of not protecting luggage against tracking.

7. Performance Analysis

For the implementation of the luggage control system, NFC tags with at least 1 KB of storage are recommended to store user data. In particular, a beta implementation of the system has used MIFARE Classic [13] tags, which have 3 KB available for user data. Note that, in this first implementation, the security of NFC tags was not a priority. The suggestion to use NFC tags with at least 1 KB of storage is based on the necessity to use keys that are secure enough for the Paillier cryptosystem. The implemented system uses two prime numbers p and q with length of 1024 bits and an integer n of 2048 bits. The largest element resulting from the system operations has 4096 bits of length, because the operations are carried out in $\mathbb{Z}_n^*$. Besides this value, a digital signature composed of a pair of values whose maximum length n must be stored too. Among the information contained in this type of NFC tags, a static field corresponding to a serial number N is the unique value in the system that cannot be encrypted. This aspect is interesting for the cryptographic system explained in Section 5 because the value N makes it possible to link the NFC tag with the passenger u and their luggage j , $u = 1, 2, \dots$, $j = 1, 2, \dots$, b_u (b_u is the number of bags of passenger u).

In order to verify the time required for Paillier cryptosystem operations, some of these have been compared using different key lengths (see Figure 8). First, the key pair generation requires the choice of two prime numbers to perform the following operations. The key generation requires most of the time because both primes must be long enough to guarantee security of the scheme. As seen in Figure 8, the search of both prime numbers spends around the 55% of time of all the operations of the system. When the primes have been obtained, the rest of the operations to obtain both public and private keys only use a low percentage of the total time. The key generation is a step that is only executed in some situations like generation of flight keys or renovation of airport keys. Thus, more than 60% of the time spent in the operations shown in the chart is not consumed

FIGURE 8: Paillier cryptosystem measurements.

at the control points. Besides, the decryption operation is shown in the chart but that is only required when an anomaly appears within the normal flow of the luggage. However, it is an operation that hardly consumes time, less than a second in the worst case.

As for the encryption and addition operations, which are the most commonly used at control points, in tests performed with large random numbers, encryption consumes roughly the same time as decryption, but addition is almost instantaneous. The time required to encrypt and add is only 100 milliseconds for a key length of 1024 bits, which is the length used in the beta implementation of this work. For this reason, these operations could be used at the control points without affecting the normal flow of luggage.

In addition, for speeding cryptographic operations, it is necessary to consider how fast NFC tags are read and written. In the current NFC standards, data rates are set to 848 kbit/s, but this speed could be greatly increased with a new implementation of the protocols described in [13]. Regardless of the speed increase, the application can write a maximum of 3 KB of data in the NFC tag. Thus, considering the low speed of 848 kbit/s, which is equal to 106 kb/s, the read and write operations are also completed instantly.

8. Conclusions

This work describes a proposal for the permanent baggage tagging that provides the ability to add new information along the control points to accelerate passenger flow and establish more security over baggage control. To the best of our knowledge, no complete tracking of luggage from the origin to the destination is contemplated in any existing system or in previous proposals. This secure and continuous tracking is here possible in practice thanks to the use of homomorphic cryptography. Besides, NFC technology is used in the proposed system because it is becoming more accepted and economically affordable. Thus, the proposed

technology can be used to provide more control, efficiency, and security in the handling of luggage at airports around the world. On the one hand, it represents an answer to the high number of complaints for delays caused by luggage check-in and loss. On the other hand, the system might provide greater protection against terrorist attacks because it involves a continuous and better baggage control. This does not mean that the system can be used to prevent this type of attacks, but the probability of detecting anomalies in the normal flow of luggage is greater thanks to its implementation. This is part of a work in progress, where a beta implementation with insecure MIFARE Classic tags has been developed. Thus, research on more secure NFC tags to manage access to information, such as MIFARE Plus, is a goal that keeps this work open.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research is supported by the Spanish Ministry of Economy and Competitiveness, the FEDER, and the CajaCanarias Foundation, under Projects TEC2014-54110-R, RTC-2014-1648-8, MTM2015-69138-REDT, and DIG02-INSITU.

References

- [1] D. Fodness and B. Murray, "Passengers' expectations of airport service quality," *Journal of Services Marketing*, vol. 21, no. 7, pp. 492–506, 2007.
- [2] D. C. Wyld, M. A. Jones, and J. W. Totten, "Where is my suitcase? RFID and airline customer service," *Marketing Intelligence & Planning*, vol. 23, no. 4, pp. 382–394, 2005.
- [3] Amadeus: Reinventing the airport ecosystem, a new airline industry report, 2012.
- [4] RP1740C, I.R.P.: Standard for RFID baggage handling, 2007.
- [5] W. Suparta, "Application of near field communication technology for mobile airline ticketing," *Journal of Computer Science*, vol. 8, no. 8, pp. 1235–1243, 2012.
- [6] O. R. Curran, L. Fischer, D. Pérez et al., "Aviation security in a digital age: can security benefit from wireless communication technologies in passenger air transport?" in *Proceedings of the 3rd International Air Transport and Operations Symposium 2012*, p. 44, 2012.
- [7] R. Boden, "British airways to offer NFC luggage tags," *NFC World*, 2013.
- [8] P. D. DeVries, "The state of RFID for effective baggage tracking in the airline industry," *International Journal of Mobile Communications*, vol. 6, no. 2, pp. 151–164, 2008.
- [9] G. E. Vastianos, D. M. Kyriazanos, V. I. Kountouriotis, and S. C. Thomopoulos, "An RFID-based luggage and passenger tracking system for airport security control applications," in *Proceedings of the Signal Processing, Sensor/Information Fusion, and Target Recognition XXIII*, vol. 9091 of *Proceedings of SPIE*, International Society for Optics and Photonics, Baltimore, Md, USA, May 2014.
- [10] C. Gentry, *A fully homomorphic encryption scheme [Ph.D. thesis]*, Stanford University, 2009.
- [11] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology—EUROCRYPT '99*, vol. 1592 of *Lecture Notes in Computer Science*, pp. 223–238, Springer, Berlin, Germany, 1999.
- [12] E. Haselsteiner and K. Breitfuß, "Security in near field communication (NFC)," in *Proceedings of the Workshop on RFID Security*, pp. 12–14, Graz, Austria, July 2006.
- [13] C. Patauner, H. Witschnig, D. Rinner, A. Maier, E. Merlin, and E. Leitgeb, "High speed RFID/NFC at the frequency of 13.56 MHz," in *Proceedings of the 1st International EURASIP Workshop on RFID Technology (RFID '07)*, pp. 5–9, 2007.