International Journal of Scientific Engineering and Science
Volume 3, Issue 5, pp. 36-42, 2019. ISSN (Online): 2456-7361

Development of Embedded IoT-Enabled Database Management System for Improved Hotel Room Reservation Accountability

Jeremiah T. Wosu[1], Gordon C. Ononiwu[2], Trust C. Oguichen[3], Obinna Opara[4]
[1, 2, 4]Dept. of Electrical and Electronic Engineering, Federal University of Technology, Owerri, Imo State, Nigeria
[3]Dept. of Electrical Engineering, Rivers State University, Port Harcourt, Rivers State, Nigeria

***Abstract*— This paper applies IoT and embedded system technologies in enforcing accountability of generated funds from hotel room bookings and reservations. Accountability of funds generated as a result of booked rooms in hotels has become one of the prevailing challenges encountered by hotel owners in recent time. This challenge, which is as a result of compromise of integrity of stored data, is responsible for loss of huge amount of money and data annually in hotel management. In a bid to curb the challenges posed by compromise of integrity of stored data in hotel room bookings and reservations, this work utilized inexpensive and off-the-shelf materials such as Raspberry pi 3B+, Arduino Nano with Atmega 328p microcontroller, ESp8266 Wi-Fi Module, ES-130B keyless door lock, and MPR121 keypad in the development of an improved database system. The system wirelessly communicates with an automated door locking system in order to allocate rooms to customers upon successful booking. Object-Oriented System Analysis and Design technique in combination with Rapid Application Development (RAD) methodology were adopted for the modeling and development of the prototype system used in demonstrating the purpose of the research. The prototype system automatically generates door access-codes for customers upon successful room booking as well as keeps track of all booked rooms and associated funds. After analyzing the degree of security of the developed prototype system against already existing hotel front office software (FOS), it was observed that the prototype system has a better performance in terms of data integrity, confidentiality, and authenticity. This obviously indicated that the stored data in the prototype system are better secured in that additional layer of security was added to the system through the application of the embedded IoT framework. Consequently, this resulted to the generation of stored room booking data with significantly reduced tendency of compromise by hotel staff or any other entity. This resulted to increased accountability and improved fraud mitigation.*

***Keywords*— IoT Embedded System; DBMS; FOS; Security; Smart Hospitality.*

I. INTRODUCTION

A. Background Study

Despite the use of sophisticated DBMSs by many hotels in managing business processes associated with room reservations, ensuring the integrity of data and authenticity of staff who access and manipulate these data have proven to be serious challenges encountered by the hospitality industry[1]. Compromise of the integrity and consistency of stored data oftentimes leads to fraud which in turn results in most hotels loosing up to 10% of their annual income [2]. According to the investigation carried out in [3], there are three possible ways in which the integrity of data associated with hotel room bookings could be compromised. These are;

i. *Compromise of funds generated at the FOS;* this often occurs when the front office manager fails to record a booked room in which payment has been made by cash. Instead, the room revenue for the guest is transferred to the folio of another guest who had already paid with card.
ii. *Compromise of room types:* in this case, if a guest initially books a room type of lower fee and later approaches the receptionist for upgrade to a room of higher standard with higher fee; the receptionist reallocates the room to the guest, collects a higher fee, and in most cases, fails to record the upgrade.
iii. *Sale of out of order rooms:* most times, rooms that are out of order rooms (such as complimentary rooms) are issued for cash and the revenue not accounted for.

To tackle these challenges, a keen and pervasive focus on revenue management is important, considering the economic effect it has in the success of every hotel. Although every hotels may adopt different mechanism in managing data regarding room bookings and associated funds, it is essential to have a well-defined and measurable strategy to enforce accountability [4]. This paper attempts to address the challenges encountered by hotel owners with respect to accountability of room bookings by adopting embedded IoT technology in reinforcing integrity of stored data in already existing hotel DBMS. It is important to state at this point that focus is given to the security of the gathered and stored data and not the IoT system itself.

The developed prototype system in this research enforces integrity of data and constrains users from compromising the originality of records (funds) relating to room reservations by applying an embedded IoT framework. The prototype system automatically generating pass codes which are used to access room doors upon successful booking. The system manages booking by recording the details of customers, hotel staff, hotel rooms, room prices, amount paid, mode of payment, mode of booking and booking durations for each reservation made. Thus, major entities involved in room bookings as well as the security of stored data are optimally monitored and kept on track. Different aspects of the stored data as well as operations used for their manipulations are made available to different categories of the hotel staff. For instance, the CEO has access to the secured data relating to room bookings and associated funds which can neither be altered by the manager nor any other user. This further enforces accountability as organizational bureaucracy is implemented in the DBMS, thereby making each and every member of the hotel staff (including the customers) to be responsible for the activities they carry out with the system. In this light, it makes it easier for the CEOs and Accounting officers to audit the financial operations of the hotel in a better secured pattern.

B. Research Contribution

This research attempts to mitigate fraud associated with funds generated in hotel room bookings by incorporating an embedded IoT framework into an already existing room booking process of a hotel. This however, was achieved by utilizing inexpensive and open-source materials like Raspberry pi 3B+, Arduino nano with atmega328p v3, ESp8266 Wi-Fi module, ES-130B keyless door lock, and MPR121 keypad in developing the prototype system. Object-oriented systems analysis and design was applied in understudying the already existing hotel DBMS. This accounted for affordable and easy implementation, and also facilitated cross-platform independence and ease of interfacing with already existing technology.

The remainder of this research is structured as follows. Section II discusses works related to the application of IoT and embedded system technologies in curbing fraud in the hospitality industry. Section III presents the basic architecture of the system in which the fundamental operations were captured. Results were presented and discussed in Section IV. Finally, the research was drawn to conclusion with recommendations in Section V.

II. Review of Related Works

As initially stated, no research in the past has directly utilized embedded IoT technology in curbing fraud relating to hotel room reservations and associated funds. As such, literatures reviewed herein are those associated with the use of IoT in the hospitality industry in relation to keyless door lock technology, front-office process automation, electronic/remote room booking, state of occupancy of hotel room, and self-service technology.

The research carried out in [6] explores the promises of IoT in future hospitality services such as body area sensors, energy management, building automation and monitoring, as well as augmented reality and beacon technology. For the process automation and monitoring which is pertinent to the research, it was pictured that new hospitality services like keyless entry service, digital doorkeeper; automated check-in and check-out services, etc. will be implemented using IoT which will bring about optimal customer satisfaction. Moreover, this will improve the operational and managerial efficiency as in-room monitoring systems can be used to detect whether a room is occupied or not in order to properly program housekeeping services, the research added.

Despite the promising prospects of IoT earlier mentioned, the research identified some associated challenges which if not properly handled, will hamper the possibility of sustainable technological development in the hospitality sector. These challenges include; interoperability, security, privacy, data management, and responsiveness.

The authors in [7] established the need for a Platform as a Service (PaaS) solution combined with an in - room IoT control system which may be controlled by a loyalty mobile app. This will track guest location as to enhance customized guest experiences and improve revenue generation. Thus they developed a system for customizing hotel rooms, conserving resources and detecting occupancy status by using a layered in – room PaaS system with an IOT network control module configured to control a plurality of IOT connected room devices.

In order to achieve their objectives in accordance with the present invention, the authors developed the following sub-systems:

i. A PaaS-based system,
ii. A room-based IoT network which includes a base module configured to control a plurality of peripheral network devices,
iii. A mobile application which is separately downloadable or embedded within an existing hotel brand app running on the guest's mobile device. The app can be configured to interface with and control the IOT network so as to coordinate hotel services,
iv. Allocation tracking service which is managed by the app and configured to monitor the location of the guest on and/or off the hotel property, and
v. A machine learning engine configured to augment the location data with contextual awareness.

As reported in [8], the research evaluates recent advancements in technology for providing security mechanisms and subsequently enforcing integrity in a network of embedded control devices such as those associated with the interaction between small firmware and heavyweight Supervisory Control and Data Acquisition (SCADA) clients and servers [9]. The main focus of the research was on the property of system integrity of Remote Terminal Units (RTUs) which is used to establish trust throughout the network. Integrity in this case was focused on the communicating IoT devices rather than the data captured by these devices. Trust in this context simply means “a device that will behave in a particular manner for a specific purpose” as defined by the Trusted Computing Group [10]. This however implied that the system would function as planned by the developer. Embedded systems security technologies such as remote attestation and privileged-based mechanisms were employed.

In [11], a mobile digital key for guestroom entry was designed and developed using a mobile phone application. The purpose for this was to speed up and optimize the efficiency of the check-in and check-out operations. It was however reviewed that some hotels adopt mechanisms such as using self-service applications with self-service technologies (SSTs) to enhance check-in operations and access control. Also, self-service kiosks (SSKs) were also developed in order to reduce customers’ waiting time on the queue [12] in [11]. However, the degree of security of data gathered as a result of room reservations and bookings was not considered. This will, as a matter of fact, give room for easy compromise of stored data which will not be noticed.

In [13], a system was developed for determining the occupancy state of a room based on a composite analysis of the state of the room door, motion activity within the room or rooms, and the location of a mobile device. The system comprises of one or more intelligent door lock module, a motion sensor which may also have some built-in intelligence, a mobile device, a software system for controlling the transmission of a message between the setback controls system and the mobile device, a software system for controlling the transmission of a message throughout the multi-room facility, and finally, a service terminal software for a handheld programmer unit. The door lock was adapted to send a wireless message to the controller each time the door is opened, detailing that it is a door-open command, opened by key or from the inside, and if by key sends the user type (guest or staff) and expiration date if it is a guest key. The door lock also sends a message when the door is closed.

In [14], engineering approach was applied to achieve a unified hotel access control system (UHACS) for seamless hotel check-in and room access. It was established that recent technological advancements have led to the emergence of an innovative, strategic solution which is the concept of keyless systems. A keyless system fulfills the functions of traditional key-enabled systems, such as granting authorized users access (e.g. by unlocking the system) to what is protected by the system (e.g. possessions or a room) without the need for original equipment manufacturer keys. Instead, a keyless system generates a unique identifier (e.g. code) that is sent directly (e.g. email or mobile application) to authorized users (e.g. hotel guests), who can then use the identifier on an existing user platform (e.g., printouts or Smartphone) to gain access [15][16].

In an article published by IT News Africa [18], it was highlighted that Enterprise Resource Planning (ERP) software could be used in prohibiting unauthorized access to internally stored data in corporate organizations. According to this article, it is believed that employees of an organization (hotel for instance) are the major risk factor for fraud in that not all employees are honest. The system discussed in this report, which was developed by Bluekey Software Solutions [19], was solely software-based. This posed the limitation of being unable to ascertain the correct status of a room so as to know when a room is actually occupied or vacant. Nevertheless, approaches such as those adopted in [14], [15], and/or [16] could have been used to achieve this.

C. Research Gaps

From the related literatures reviewed so far, the following gaps have been identified with respect to using embedded IoT in mitigating fraud in the hospitality industry:

i. Embedded IoT technology has not been applied in enforcing integrity of stored data in hotel DBMS in order to reduce fraud in room bookings.
ii. Appropriate software engineering principles and patterns have not been adequately applied in developing fraud reduction/elimination system for hotel room reservations using embedded systems and IoT technology.
iii. The real-time properties of entities constituting of the hotel DBMS have not been adequately considered as factor for checkmating and enforcing data integrity and consistency.

D. Research Objectives

i. To evaluate the procedures involved in hotel room bookings and reservations; and determine possible causes of fraud in hotel management.
ii. To model the system by adopting object-oriented system analysis and design techniques.
iii. To develop an embedded IoT system that enforces access control in hotel door locking systems.
iv. To develop a web application and a secured database for checkmating the integrity and confidentiality of data relating to hotel room allocations and associated funds.
v. To build a prototype system by integrating the embedded IoT system and with the web application and secured DBMS.

III. Design Framework/Architecture

The prototype system is generally divided into four hardware modules namely;

i. The door – which is situated at the entrance of every hotel room – consists of ES-130B keyless door lock and MPR121 keypad controlled by Arduino nano with atmega328p v3,
ii. A raspberry pi 3B+ – which serves as a central controller containing the ESp8266 Wi-Fi module,
iii. Client machines (desktop, laptop, tablet and Smartphone) – which run a dedicated web application for making bookings, and
iv. Cloud data storage server – which serves as the database for storing all related data concerning room reservations and associated funds. Furthermore, a monitoring tool was developed to enable the supervision of all the activities that take place in the DBMS.

The QHWES-130B keyless door lock is made up of stainless steel and has a dimension of 160x25x31mm. It operates on a voltage of 12V with a DC supply of 200mA.

The MPR121 keypad is composed of twelve sensitive pads with an I^2C (inter-integrated circuit) output. The MPR121 functions by measuring the capacitance of twelve electrode points. Whenever an object is placed close to the electrode connector, the capacitance changes, thereby signaling the keypad that something has pushed a button.

The raspberry pi 3B+ runs on a 64-bit quad-core ARM Cortex-A53 processor with a clocking speed of 1.4GHz. It has 1GB RAM, a dual-band 802.11 wireless LAN, Bluetooth 4.2, and a 300Mbits/s Ethernet.

An inexpensive webhosting company [20] was used as a cloud storage platform for storing the data that are gathered using the client machine(s) as depicted in the system architecture (*see figure 1*). After logical design of the database (by using object-oriented system analysis and design approach), the data logic and data access logic was implemented using the C# Asp.net programming language in Microsoft Visual Studio Integrated Development Environment and deployed to the cloud host.

The interaction between the components of the system is depicted in figure 1 below;

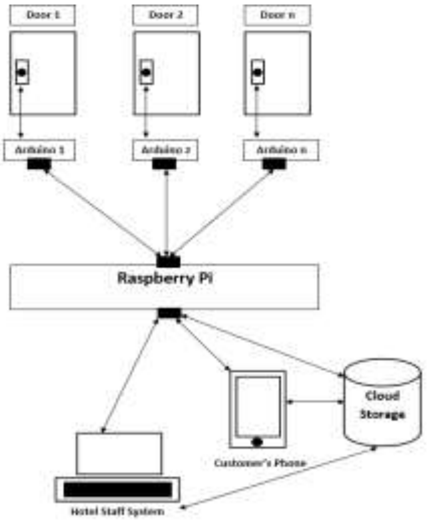

Fig. 1. System Architecture

The Raspberry pi 3B+ which acts as the central controller of the entire system is responsible for the generation of access-codes. These codes are transmitted wirelessly to the ESp8266 Wi-Fi modules attached at each door, which are embedded with Arduino nano (atmega328p v3). The Arduino nano then updates the secret code in its memory. This secret code is used to unlock the door when matching code is keyed into the system via the keypad by a user (customer or hotel staff). The raspberry pi also updates the database with the auto-generated access-code via attached internet module. This communication is achieved through a dedicated TCP/IP port.

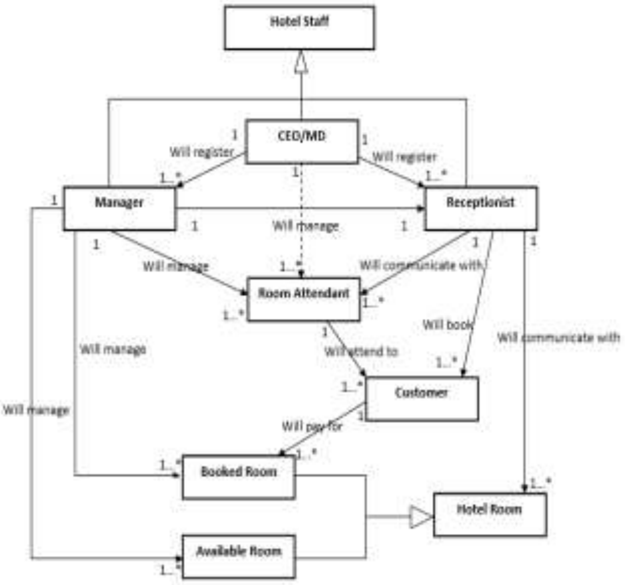

Fig. 2. System Class Diagram

The client machine which can be a desktop, laptop, tablet, or Smartphone runs a dedicated web application developed for the hotel customers and staff to use in making room bookings. The web application interacts with the cloud storage server and the central raspberry pi controller as depicted in figure 1.

Considering that object-oriented system analysis and design approach was used to model the hotel DBMS in order to facilitate easy and efficient enhancement, figures 2 are used to represent conceptual data model respectively.

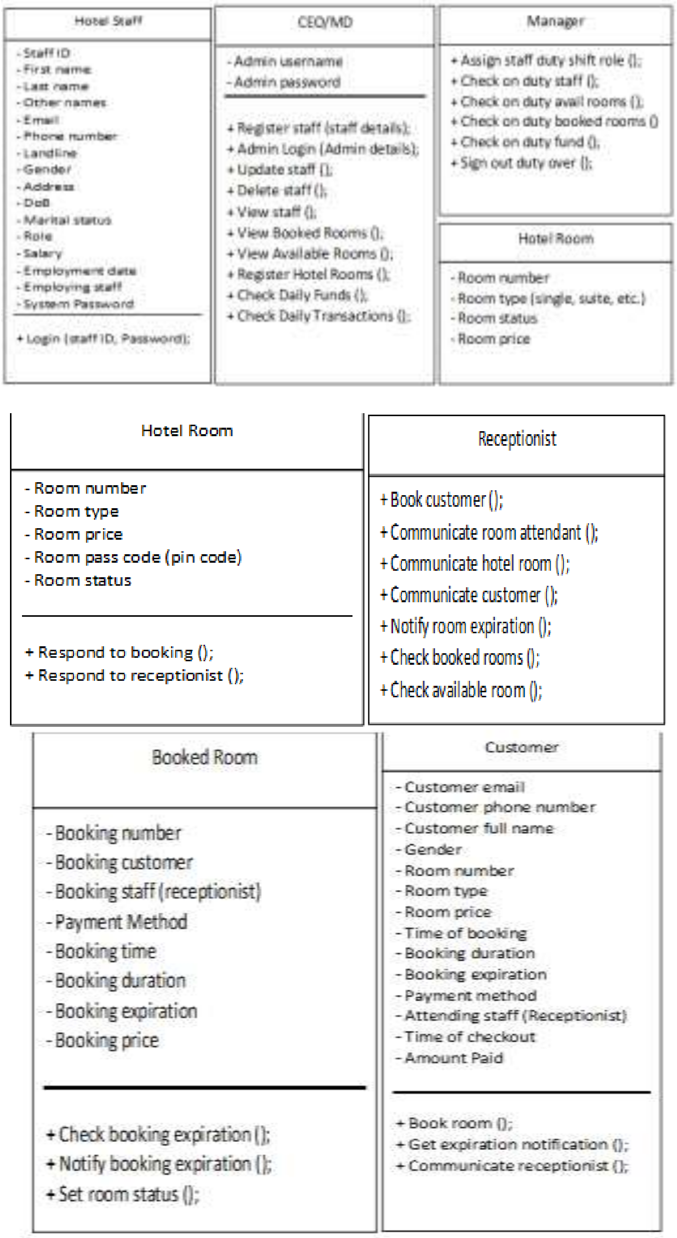

Fig. 3. DBMS Objects, Attributes, and Operations

Figure 3 above shows the UML notation of attributes and operations of each of the database objects (which eventually became tables upon implementation) [21]. This gave a clear insight of how data are stored and the interrelationship between them in the DBMS. Objects in the database communicate with one another using their operations via a mechanism called message passing [22].

This approach further enforces encapsulation of data, modularity, polymorphism, data abstraction, as well as atomicity; features deemed very important in the security and maintainability of data in a relational DBMS.

IV. Results and Discussion

Considering the nature of this research which is focused on securing data in a hotel DBMS by applying embedded IoT technology to enhance accountability; integrity, confidentiality, and authenticity of data stored were considered the key parameter indices (KPIs) for evaluating the system. Nevertheless, from discussions so far, it is obvious that these parameters are of utmost importance to data security in DBMSs, and consequently, fraud mitigation in hotels with respect to room bookings and reservations.

The developed prototype inherently enforces integrity of stored data considering that object-oriented analysis and design approach adopted in modeling the system. Moreover, the adopted IoT and embedded system technologies added extra layer of security by providing real-time access control and coordination of interaction of entities that make up the entire system. It is also important to state at this point that delicate data fields such as room door access-codes, room prices, and details of hotel staff associated with each room reservation were automatically generated thereby eliminating the possibility of compromising authenticity, integrity, and confidentiality of data.

The developed prototype system was tested against an already existing automated management system used by a local hotel using the KPIs earlier identified. The degree of data compromise which determines the extent to which the entire system is exposed to fraud was tested against the progressive increase in the number of room bookings for the already existing system at first. Thereafter, it was tested for the developed prototype system. Progressive increase in the number of room bookings was used as a determinant as increase in the number of customers who visit and make bookings with the hotel leads to increase in generated funds and thus, increase in the tendency of financial crime.

According to [23], [24] and [25], confidentiality, integrity, availability, and authenticity are key security requirements that must be met for data to be safe. Confidentiality of data simply refers to the protection of data from unauthorized users; integrity simply means that data that are stored in the DBMS should not be altered and if at all there is a need for modification, should be done by only authorized persons; availability requires that data are available to authorized users whenever needed; and lastly, authenticity is the ability of the system to verify the identity of the user in order to control who gets access to what data.

With respect to the proposed system, it is an essential requirement that the stored data in the hotel DBMS be kept strictly confidential from unauthorized access. In this case, if the duty of a receptionist is to book customer and communicate with hotel room as depicted in the conceptual data model (*see figure 2)*, then the receptionist should not be authorized to have access to data regarding to staff registration and deletion.

In terms of integrity of data, the persons who have access to the DBMS should have little or no permission to alter data that are stored in the database. This means that if a total of twelve rooms were booked, amounting to a specific amount, for a day, for instance, then neither the number of rooms booked, nor the amount generated should be altered. As such, delicate data of this nature are generated automatically and WRITE permission disabled on them.

The percentages of data integrity, confidentiality, and authenticity were used to obtain the degree of security of the system. This implies that the degree of security of the system directly depends on the percentage of data integrity, confidentiality, and authenticity as shown in equation 1 below;

$$degree\ of\ security = (\%integrity) + (\%confidentiality) + (\%authenticity) \quad (1)$$

These percentages were tested against the number of bookings (single rooms to be specific) made for different days. The number of rooms booked were intentionally increased by a factor of 10 for ten days. A total number of ten hotel staff (with different levels of authority) were also allowed access to the hotel DBMS for the ten days. The parameter '*Number of bookings'* was used to test against degree of security (*shown in equation 1*) due to its significance to funds generated in hotel. It is believed that the higher the number of bookings, the higher the fund generated, and consequently, the higher the tendency of fraud in the system.

The percentage of data integrity was obtained by dividing the actual amount generated by the expected amount to be generated and multiply the result by 100%. Mathematically,

$$\%\ Integrity = \frac{A_a}{E_a}\ X\ 100\% \qquad (2)$$

Where A_a = Actual amount realized, and
E_a = Expected amount that ought to be realized.

For example, if it is registered that a single room is booked for N 10 per night, then if 10 rooms are booked;
Expected amount = N 10 x 10 rooms = N 100
If the actual amount is eventually = N 95,
Then the percentage integrity is thus;
□ % integrity = (95 ÷ 100) x 100%= 95%.

For the percentage confidentiality, it is important to recall that a monitoring software tool was incorporated into the DBMS (*see section III*) which was used to supervise activities pertaining interactions between entities in the database. At default, it is assumed that all the stored data are confidential from unauthorized access. In this case, the confidentiality of the system is set to a default value. As the number of booking increases, the tendency of users accessing data they are not authorized to access increases. Whenever this occurs, the supervisor tool records the number of unauthorized access. As this occurs, the confidentiality value decreases. Mathematically,

$$\%\ Confidentiality = \frac{D_c - N_d}{D_c} X\ 100\% \qquad (3)$$

Where D_c = Default confidentiality, and
N_d = Number of unauthorized access to data.

The same reasoning for obtaining percentage confidentiality was applied for authenticity. Here, the monitoring software tool was set to check the number of unauthorized users that access the system. At default, the authenticity value of the system is set to a value, as the number of unauthorized access increases, the percentage of authenticity of the system decreases. Therefore, mathematically,

$$\% \, Authenticity = \frac{D_a - N_s}{D_a} \, X \, 100\% \qquad (4)$$

Where D_a = Default authenticity, and
N_s = Number of unauthorized access to the system.

From the discussions thus far, in order to effectively curb fraud in hotel DBMSs with respect to room reservations and bookings, the degree of security of the stored data must be high. This is in order to effectively mitigate the ease of compromise of stored data from the hotel staff such as receptionists, room attendants, manager, as well as hackers. In this case, high percentage of data integrity, confidentiality, and authenticity of the entire system must to a great extent be maintained.

The results for the already existing and developed prototype system are shown in tables 1 and 2, and represented in figures 4 and 5 respectively below;

TABLE 1. Relationship between number of bookings and security of data i.e. Daily generated fund (in terms of confidentiality, integrity, and authenticity) for the already existing hotel booking process.

No of Bookings	Data Integrity (%)	Data Confidentiality (%)	Data Authenticity (%)
10	99	100	100
20	75	97	87
30	60	95	85
40	52	92	80
50	54	82	78
60	40	70	75
70	21	64	70
80	10	45	63
90	9.8	40	31
100	20	20	20

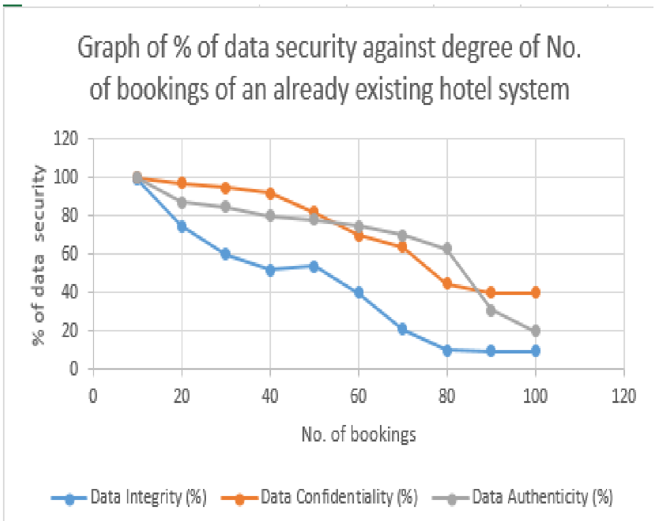

Fig. 4. Test result for an existing system

TABLE 2. Relationship between number of bookings and security of data i.e. Daily generated fund (in terms of confidentiality, integrity, and authenticity) for the prototype system.

No of Bookings	Data Integrity (%)	Data Confidentiality (%)	Data Authenticity (%)
10	99	100	100
20	97	100	100
30	95	100	100
40	92	98	100
50	85	97	98
60	84	96	96
70	82	93	97
80	80	93	95
90	80	93	95
100	80	93	95

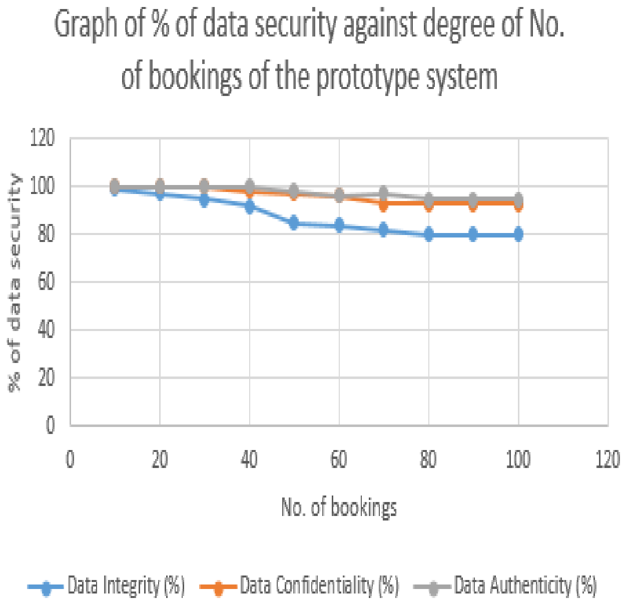

Fig. 5. Test result of prototype system

From the results of the already existing system (see figure 4), it is obvious that there is an exponential decline in the percentage of security of data as regards integrity, confidentiality, and authenticity as the number of bookings increases. On the contrary, the drop in the percentage of data security for the prototype system is virtually insignificant. The object-oriented modeling of the prototype system DBMS resulted to the optimal organization, storage, and operations of stored data. However, the minimal drop in the percentage of data security associated with the system is mainly attributed to the adoption of IoT and embedded systems which not only provided seamless coordination of the associated cyber-physical systems, but also improved the integrity, confidentiality, and authenticity of data by enforcing some levels of constraints.

The system provides different interfaces, access rights, and privileges to different categories of users. These categories include the customers and all level of hotel staff as indicated in the conceptual data model (*see figure 2*). These interfaces provide different access to different data as well as operations for manipulation of these data. For example, a CEO/MD can access data relating to room reservations and funds generated which can neither be distorted by any member of staff nor unauthorized persons. In view of this, it is easier for the CEOs and Accounting officers to audit the financial operations of the hotel in a better secured and professional manner.

V. Conclusion and Recommendation

This research applied IoT and embedded system technologies to mitigate internal fraud in hotel room reservations and its associated funds. By so doing, room booking process has been made smarter and more efficient as the security of generated data has been enhanced and the interaction between the users and booking procedure improved. Object-oriented system analysis and design were applied in understanding and modeling the behavior of already existing hotel room reservation process. Inexpensive and off-the-shelf materials were used in the development of a prototype system which resulted in the drastic reduction of implementation cost and easy integration of the system to already existing business process. Furthermore, the prototype system was tested against an already existing hotel management system to examine how the number of bookings influence the degree of security of stored data in terms integrity, confidentiality, and authenticity. In this regard, results have proven that the prototype system out-performed the already existing system. It also proved to be more scalable and efficient in terms of handling large amount of data as increase in number of users did not significantly affect the system operations.

In the future, it is recommended that multiple raspberry pi microcontrollers be used in order to enhance the processing speed and concurrent execution of operations of the system. This will account for parallel execution of tasks, thereby resulting to better system performance. Also, fingerprint authentication mechanism can be adopted for the hotel staff. This will enhance data authenticity as well as integrity and confidentiality. Furthermore, considering the nature of this research which concerns the use of interconnected physical devices communicating over the internet through the use of embedded sensors, the security of these interconnected objects is of great concern as they can serve as potential loopholes for attack vectors. Future works should apply mechanisms such as those discussed in [26] and [27], in order to protect the embedded IoT devices from unauthorized access which might lead to malicious damage of data pertaining room bookings and other related processes as well as the entire system.

References

[1]. Wint Wah Loon, Haymar Aung, Hlaing Htake, and Khaung Tin, "Learning the Requirements Engineering Process of the Online Hotel Reservation System" International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 Volume-7, Issue-8, 2018.

[2]. Shah, S. (CPA),"Combating Fraud in the Hospitality Industry". Berdon Industry Insights. New York, 2018.

[3]. Ernst and Young LLP," Managing fraud, bribery and corruption risks in the hospitality industry". EY Fraud Investigation and Dispute Services (FIDS). India. EYIN1605-045, 2016.

[4]. www.hotelnewsnow.com/Article/8684/5-ways-to-make-accountability-easier. Retrieved from Smith, J. "Five ways to make accountability easier", 2018.

[5]. http://wireless.ictp.it/school_2015/presentations/secondweek/ITU-WORK-ON-IOT.pdf. Retrieved from Zavazava, C."ITU Work on Internet of Things" 12th October, 2018.

[6]. Prasanna Kansakar, Arslan Munir, and Neda Shabani, "Technology in Hospitality Industry: Prospects andChallenges" 2017.

[7]. Yani Deros, and Jodi Deros "Systems and Methods for Customizing Hotel Rooms, Detecting Occupancy Status and Conserving Resources Using Internet of Things Devices" 2018.

[8]. Tobias Rauter, Andrea Höller, Johannes Iber, Michael Krisper and Christian Kreiner, "Integration of Integrity Enforcing Technologies into Embedded Control Devices: Experiences and Evaluation" IEEE 22nd Pacific Rim International Symposium on Dependable Computing 2017

[9]. Zhou, X., Xu, Z., Wang, L., and Chen, K."A structured review of SCADA system cyber security standards." 2017 4th International Conference on Control, Decision and Information Technologies (CoDIT).

[10]. https://www.trustedcomputinggroup.org/ Retrieved from K. J. Biba, "Integrity Considerations for Secure Computer Systems, Tech. Rep., 1977 TCG, Trusted Computing Group," 2nd November, 2018.

[11]. Arnelyn M. Torres, "Using A Smartphone Application as A Digital Key for Hotel Guest Room and Its Other App Features" International Journal of Advanced Science and Technology (IJAST) vol.113, pp.103-112, 2018.

[12]. http://journals.sagepub.com/doi/abs/10.1177/1847979017720039. Retrieved from S. N. Cheong, H. C. Ling, P. L. Teh, P. K. Ahmed and W. J. Yap, "Encrypted quick response scheme for hotel check-in and access control system", October, 2017.

[13]. Stig Lagerstedt, Daniel Berg, Daniel Bailin, Castle Rock, Mark Robinton, Masha Leah Davis, "The Use of Motion Detectors, Door-lock State and Mobile Device Location in Determining Hotel Room Occupancy Status" 2018.

[14]. Weng Marc Lim, Pei-Lee Teh, Pervaiz K. Ahmed, Soon-Nyean Cheong, Wen-Jiun Yap, "Going keyless for a seamless experience: Insights from a unified hotel access control system" International Journal of Hospitality Management 75 (2018) 105–115

[15]. Cobos, L.M., Mejia, C., Ozturk, A.B., Wang, Y. "A technology adoption and implementation process in an independent hotel chain". 2016 Int. J. Hosp. Manage. 57, 93–105.

[16]. Egger, R."The impact of near field communication on tourism." 2013 J. Hosp. Tour.Technol. 4 (2), 119–133.

[17]. https://www.oracle.com/industries/hospitality/what-is-hotel-pms.html. Retrieved from Oracle Hotel PMS. "Delivery a Seamless Guest Experience with Hotel PMS" 10th November, 2018.

[18]. http://www.itnewsafrica.com/2010/02/intelligent-use-of-erp-can-help-mitigate-internal-fraud/IT News Africa. Retrieved from Intelligent use of ERP can help mitigate internal fraud. 30thOctober, 2018.

[19]. https://www.bluekeyseidor.com/ Retrieved from Bluekey Seidor. 4th November, 2018.

[20]. https://www.smarterasp.net Retrieved from Smarterasp.net. 28th, October, 2018.

[21]. Holger Schmidt, Denis Hatebur, and Maritta Heisel, "Developing Secure Software Using UML Patterns" 2015.

[22]. Hendrix, R., and Weeks, M. "First Programming Language for High School Students" 2018. Proceedings of Society for Information Technology & Teacher Education International Conference (pp. 1896-1903)

[23]. William Stallings, "Cryptography and Network Security, Principles and Practices" 4th Edition 2006. Pearson Education Upper Saddle Rivere Text ISBN-10: 0-13-187319-9.

[24]. William Stallings, "Data and Computer Communications" 8th Edition 2007. Pearson Education Upper Saddle River. ISBN: 0-13-243310-9

[25]. http://www.pwc.co.uk/assets/pdf/2015-isbs-executive-summary-02.pdf. Retrieved from Chester Rebeiro, "Cryptography and Network Security Introduction" IIT Madras. 8th November, 2018.

[26]. https://www.al-enterprise.com. Retrieved from Alcatel Lucent Enterprise (ALE). "The Internet of Things for Hospitality Industry: build a secure foundation to leverage IoT business opportunities"28thOctober, 2018.

[27]. Anna, K.S., Franziska, R., and Tadayoshi, K. "Securing vulnerable home IoT devices with an in-hub security manager"2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops).