Using IoT-Enabled RFID Smart Cards in an Indoor People-Movement Tracking System with Risk Assessment

Mary Jane C. Samonte*, Darwin A. Medel, Joshua Millard N. Odicta, and Ma. Zhenadoah Leen T. Santos

School of Information Technology, Mapua University, Makati City, Philippines; Email: {damedel, jmnodicta, mzltsantos}@mymail.mapua.edu.ph (D.A.M., J.M.N.O., M.Z.L.T.S.)
*Correspondence: mjcsamonte@yahoo.com (M.J.C.S.)

***Abstract*—As the COVID-19 pandemic ravaged the planet at a standstill, remote employment seemed inescapable. Still, for some businesses that rely on the on-site presence of employees, this was a lethal blow. As time passed, restrictions got looser and allowed people to strike a balance between on-site and remote work. Thus, tracking people's indoor movements for purposes involving activity inference, security, and contact tracing is more crucial than ever before. This research explores the applicability of (Radio Frequency Identification) RFID contactless smart cards in tracking people's movement within an enclosed establishment by building a proof-of-concept prototype that allows the mentioned purposes. Furthermore, the system underwent multiple test phases to verify that the system meets the functional and non-functional requirements listed to ensure the system's operational success. Consequently, the test results prove that: 1) the system is behaving as intended; 2) the system is secure from known high-risk vulnerabilities; and 3) the system satisfies user requirements and standards, thus fulfilling the functional and non-functional requirements for a human-tracking movement system.**

***Keywords*—Internet-of-Things, Radio Frequency Identification (RFID), smart card, indoor tracking system, risk assessment**

I. Introduction

People spend a lot of their time inside buildings such as homes and offices. Due to the current state of the COVID-19 pandemic, businesses are looking for ways to safely transition from operating fully online to once again work in their offices. Work environment should not sacrifice safety of their employees and customers. Thus, the tracking of people indoors is now even more relevant than before. On a different note, there is an increasing deployment of smart cards to manage identities and access in an organization [1]. Smart cards provide a means to automate authentication, providing security and efficiency. Tracking the location of people indoors and pairing it with the right system can ensure safety and security, increase productivity in offices, and assist in navigation, among other things [2, 3]. Therefore, it may be a great idea to explore how some existing systems in buildings, such as a card-based authentication system, can be used to track people's movement indoors.

Smart identification cards can streamline several everyday tasks, such as transacting with private or public organizations or verifying a person's identity [4]. Contact tracing is one of the methods used to help keep the spread of infectious diseases manageable. Contact tracing today helps slow down the spread of COVID-19 by narrowing down the list of possible sources of infection and letting people who may have been exposed to a COVID-19 infected person know about the incident. As stated by the World Health Organization (WHO) [5], an excellent systematic application of contact tracing will "break the chains of transmission" of COVID-19 and other infectious diseases and should thus be used by the public in the event of an outbreak of a disease.

Traditional contact tracing is often done by calling and manually notifying individuals who test positive for the disease and the people with whom the infected individual has come in contact [6]. This method is inefficient because it depends on the infected individual's memory and may not give clear or complete details. Some places use logbooks that contact tracers can look at to help them trace the whereabouts of an infected individual [7]. As an attempted solution, several forms of technology were proposed, developed, and deployed. However, some of the digital contact tracing solutions' methods were either faulty or lacking [8, 9].

Smart cards have seen a steady increase in use globally, more and more smart cards have made their way into people's wallets due to their wide variety of applications in transit, IDs, and payment methods. One particular function of smart cards is to serve as identity tokens to support identification and authentication in an organization. However, some infrastructures that support smart card deployment were often developed ad hoc [10]. Furthermore, as the COVID-19 pandemic runs its course, digital contact tracing systems were designed using various approaches. Some addressed the limitations of the other solutions, from automating the traditional paper-based approach to contact tracing utilizing IoT, Bluetooth,

Manuscript received May 10, 2022; revised July 30, 2022; accepted August 30, 2022; published March 8, 2023.

and cellular network technologies. However, the problem with the inclusivity of people who do not have the technical requirements is yet to be addressed [11]. This study aims to present the development of a system that uses a Radio Frequency Identification (RFID) contactless smart card system that could track the movement of humans in an establishment. The developed system provides an additional layer of security, enables activity inference, and serves as a means to provide an alternative contact tracing method to supplement the existing contact tracing processes. The developed contact tracing system includes the following: an RFID smart card scanner; a web-based application for all users' interface; a database to store user accounts, preferences, configurations, and other related data; and the backend infrastructure for connection of all the components.

II. Review of Related Literature

The study of Chandramouli [10] discusses the prominence of smart cards being used as identity tokens to support identification and authentication in an organization. However, many of the existing infrastructures supporting smart card deployment are designed in an ad hoc manner. Consequently, the author developed a design methodology for Infrastructure System for Smart Card Deployment (IS-SCD) based on business processes, security principles, and the functional requirements of government smart card specifications adopted for large-scale deployments [12].

The study of Polenta *et al*. presented the use of a Bluetooth-utilizing dedicated IoT device for contact tracing to attempt to boost the initial adoption of their proposed system [12]. The authors explained that a smartphone performing the same task as their dedicated device would have its battery drained faster, thus disincentivizing the use of a smartphone-based system. Furthermore, they claimed that the dedicated device could be used in places or situations where users would not bring a smartphone.

Rahman *et al.* suggested using mobile phone networks as an alternative to Bluetooth-based approaches to contact tracing [13]. The authors mentioned that the approach to proposed contact tracing would require only a phone with an active SIM card and based on geolocation, thus eliminating the technological requirements and issues associated with Bluetooth technology. The geolocation data will be determined by directly acquiring location data from a cellular base station. To measure the impact of their proposed method, the authors compared it with existing Bluetooth-based approaches. It counts how much exposure a contact tracing process involving only smartphones can detect versus their proposed contact tracing process involving all phones, including feature phones.

III. System Design and Development

The developed system is named "KontaKard," which includes a smart card scanner, a web application, and a backend infrastructure. The contactless card scanner was made using an Arduino microcontroller board and an RC522 RFID module. The Arduino microcontroller provided an Internet connection using either a Raspberry Pi computer or an ESP8266 ESP-01s Wi-Fi Module for Arduino. A W5100 Arduino Ethernet Shield with an ethernet cable demonstrates its flexibility and ability to adapt to either wired or wireless connectivity needs. Mifare Classic 1k RFID cards were used for the card prototype [14]. Aside from that, the transmission of data from scanners to the server is encrypted with Transport Layer Security (TLS). This effectively protects from possible snoopers and thus provides privacy and security. The web application was built with Laravel and Vue.js with a MySQL database. Also, a Python script was added to enable the communication flow between the scanners, the central server, and the user interface.

The system presents an interface for the different access authorities. Location and movement are visible to the viewer, who could then make inferences. However, the contact tracing functionalities of the system provided an automated analysis by showing heatmaps and sending out notifications to close contacts. There are user accounts for regular users, separate from the accounts of people with a higher level of privilege. The Department of Health (DOH) [15] provided the guidelines on contact tracing of confirmed Coronavirus Disease (COVID-19) cases. The policy defined a close contact if there was a chance they may have come into contact with probable or confirmed infected people within two days before the infected person/people's diagnosis until they (the close contact) test negative for the disease. The appropriate columns in the database, such as user passwords, are hashed using the salted Bcrypt hashing algorithm.

The system caters to three users: regular users, health professionals, and administrators. The primary difference between the three users is that the health professionals and administrators will have access to particular parts of the web application that allow them to perform actions that regular users cannot do. Health professionals are permitted to register any COVID-19 positive individual to the system. This feature is necessary for the system to conduct contact tracing and view the diagnosis reports in the system. Administrators also have access to the same diagnosis reports, a list of the cards in the system, and various special functions across the application that allows them to configure certain parts of the system, including the users' information. It is part of the administrators' responsibilities to set up the system to fit the floor plan associated with the organization's building. They are to input a link to an image of the floor plan with acceptable formats only and then add the necessary rooms and scanners.

Health professionals are tasked to record infected individuals; then, the system will generate notifications at varying levels depending on exposure. The type of exposure (Very Low, Low, Moderate, and High Severity Exposure) inferred by the system will be sent directly to the appropriate users with whom the infected person has come in contact. The notifications and how it maps to the exposure case classification described by the DOH

document in the Department Memorandum (DM) 2020-0439 [16] are shown in Fig. 1(a). Updates on the dashboard are automatic using color coded exposure levels. Yellow means low exposure level, orange means moderate exposure level and red means high exposure. The severity levels of exposure for locations as shown in Fig. 1(b).

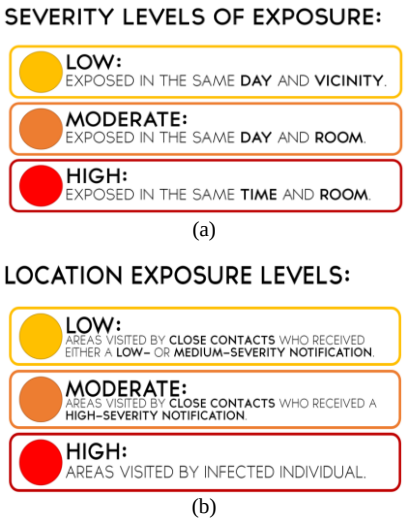

Figure 1. a) Contact tracing notification levels and b) severity levels of exposure of locations.

The dashboard of KontaKard was designed based on the GQM (Goal-Question-Measurement) model approach discussed in the study of Janes *et al.* [17], as shown in Fig. 2. First, the goal of the KontaKard dashboard was defined at the conceptual level. The dashboard provides the following information: close contacts, traced contacts, infected individuals, the whereabouts of the infected person, exposure levels of locations, inferring human activity, transactions done in a room, and rooms left unattended. Next, to characterize how the defined goals could be achieved, the questions at the operational level were defined. These include asking which places had a high/moderate/low severity exposure, who among the visitors/people who were present were infected, who among the visitors/people who were present had close contact with the infected people, or where a particular person was during a given time. Lastly, the measures in which the questions would be answered objectively were identified: diagnosis from registered health professionals and system logs from contactless smart card scanners.

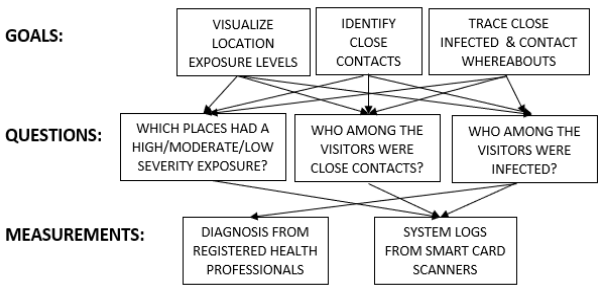

Figure 2. KontaKard's dashboard GOM model.

The dashboard features two types of data: contact-tracing-related data and general movement-tracking data. Both figures utilize the same floor plans as the base template. The floor plans are color-coded and designed according to the location exposure severity levels and the whereabouts of the people inside the building. The sample dashboard contents are shown in Figs. 3–5. The rooms being evaluated can be selected, a floor map is also displayed and there is an interface for contact tracing notifications.

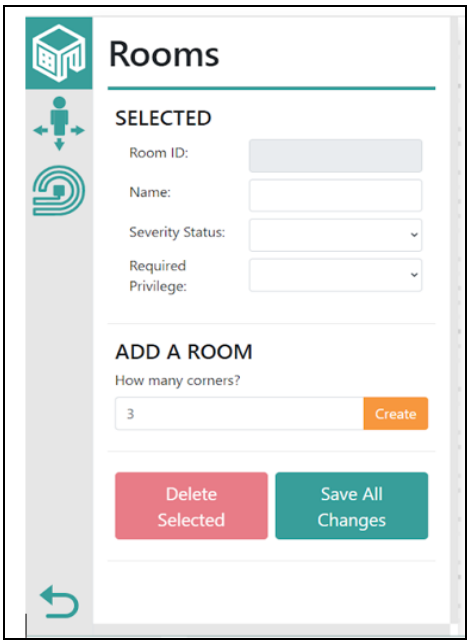

Figure 3. The room assignment in the dashboard.

Details about the people on the map can be revealed by hovering over the person-shaped symbols that indicate their presence in a particular area. The design is prepared in case members of an organization are diagnosed as COVID-19 positive. In that case, it is recommended that the organization closes down and the affected facilities conduct disinfection measures as soon as the notifications are delivered. Rules and policies are based on the government's COVID-19 Response Protocol [18]. In adherence to the minimum health standards stated in the Workplace handbook on COVID-19 management and prevention [19], a symptom-based strategy will determine if the individual is recovered or fit to work. Individuals will be marked as recovered in the system upon presenting a negative polymerase chain reaction (PCR) test. Employees are allowed to switch their RFID cards to active or non-active mode. A web-based access method is used to deactivate or activate the RFID cards for security purposes, including lost or misplaced. A report should also file to the administrator's office. This will prevent the risk of having the misplaced card misused. However, they will not be able to reactivate their card if it is disabled by a medical health professional, as previously mentioned. All users (regular users, health professionals, and admins) can participate in the automated logging process by tapping their KontaKard cards into smart card

scanners situated in establishments. This part of the process builds the necessary associations between the users and their whereabouts for the system to infer close contacts when generating notifications.

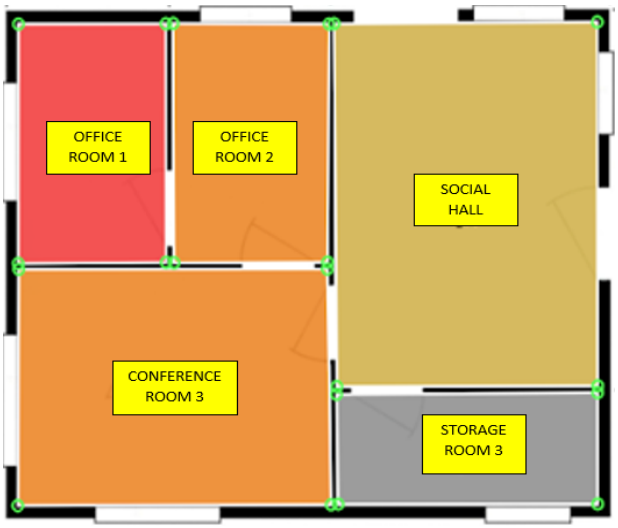

Figure 4. The floor plan mapping diagram in the dashboard.

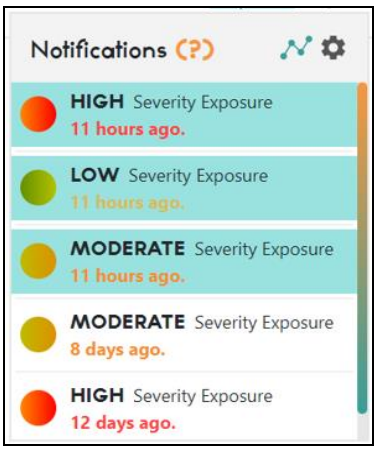

Figure 5. The contact Tracing notifications.

In the contact tracing process, if a user has tested positive, the healthcare provider updates the user's information in the system. The close contacts of the infected individuals are notified automatically by the system. In addition, notifications may automatically be sent through the web application. Lastly, the required data may be sent to the government by the system's administrator/s to comply with the standard contact tracing procedures described in the DM 2020-0189 [15]. Close contacts must be quarantined and monitored daily for 14 days or until tested negative. Probable, suspected, and confirmed cases would not be allowed to enter public establishments and transportations. The Universal Serial Bus (USB) cables connected to the Arduinos were connected to a Raspberry Pi, which transmits data to the central server hosted via Azure App Services. The initial design of the scanners is shown in Fig. 6. An auto-generated notifications in the web application is a report containing the list of infected places and close contacts was designed when a health professional diagnosed a user, whose columns were based on the Case Investigation Form [20]. The web application is built using Laravel and Vue.js [21] with a MySQL [22] database, accompanied by Python [23] for scripting.

Figure 6. Initial scanner design of KontaKard.

IV. TESTING

Every system component was tested thoroughly for defects, errors, and even vulnerabilities to be corrected before implementation. To fully capture the system's behavior and performance, the following testing levels: 1) functionality testing, this level ensures if the system satisfies the functional requirements or not; 2) usability testing, this level ensures if the system satisfies the non-functional requirements or not; 3) vulnerability testing, this assessed whether the security of the system could withstand common attacks and does not contain any known security vulnerabilities; 4) cross-browser testing – this ensured that the web application that is included in the system is functioning as intended across the most commonly used browsers; 5) Stress testing– which revealed any weakness in the system's performance and efficiency in terms of computation and processing; and lastly; 6) Acceptance testing; this evaluated the general opinion of potential users about the system and as well as contact tracing systems in general.

The study used convenience sampling; respondents were chosen based on their availability. The reason behind selecting this sampling method is the challenging nature of conducting tests during the COVID-19 pandemic, such as requiring the physical presence of users. The study had thirty-one respondents. The respondents are twenty-eight office workers, one professional IT System Administrator, and the last two are experienced Medical Technologist and a Nurse as health workers of the system.

For the usability test, the respondents were given a test that measured the usability of the developed system. The trial involved tasks that the respondents were instructed to perform. In addition, surveys were also conducted to answer after every completion of the task.

The user acceptance test survey consisted of forty-one measurement items in total, adopted from the Technology Acceptance Model in Health Informatics by Rahimi *et al.* [24], using a 5-point Likert scale (ranging from 1=strongly disagree to 5=strongly agree). The model was utilized to determine the user's thoughts and perceptions about the system, which dictated whether they were likely

to use and adapt it. The model comprises three different models, namely: Technology Acceptance Model [24], Unified Theory of Acceptance and Use of Technology (UTAUT) Model [25], and Task Technology Fit (TTF) model [26], integrated into one single model with two additional constructs.

The stress test involved feeding large amounts of data input to the system to see how it would perform compared to providing just small to moderate amounts of input data. The tool used was ApacheBench. The security compliance of the system was assessed with a vulnerability scanner (OWASP ZAP) [27] that examined the vulnerabilities of the system and determined their risk levels. The cross-browser test is essentially a checklist to ensure the web-based application's compatibility across different browsers that different users may use. Lastly, the system's functionality involved a list of output expectations, given specific data values, and then determined whether or not the system consistently produced the expected outputs when provided with data. This included determining if a particular user would receive the correct type of exposure severity notification and whether the system would mark a certain vicinity in its map with the right color.

The study utilized the TELOS approach to assess the feasibility of the developed system. TELOS stands for technical, economic, legal, operational, and schedule feasibility and is used in determining different factors of the developed system to evaluate its feasibility [28].

V. Results and Discussion

The study used a problem severity classification to analyze the usability test data to interpret the data acquired from the conducted tests. Problem severity is a combination of two factors: the impact of the problem on the functionality of the system and the frequency of the users encountering the issue during the usability test. Problem impact can be classified as high, moderate and low. A high problem impact means it completely prevents users from accomplishing the task (critical error). A moderate problem impact means it does not entirely prevent task completion but causes difficulty to the user (non-critical error). And a low problem impact means there are small issues that do not affect the task completion process in a significant way (non-critical error). The frequency of the problem is based on the percentage of participants experiencing them. A high-frequency problem was experienced by 30% or more of the participants, a moderate frequency problem was experienced by 11% to 29% of the participants, and a low-frequency problem was experienced by 10% or less. After determining the impact and frequency, the problem severity classification is derived from the two variables based on the criteria shown in Table I. A time-on-task goal for each task was created to be compared against the actual time it took each participant to finish a task. The time-on-task success rate was then calculated by comparing the two.

TABLE I. Usability Test Problem Severity Classification Based from Usability.Gov in [29]

		FREQUENCY		
		L	**M**	**H**
IMPACT	**LOW** (< 10% of the participants	4	3	2
	MODERATE (non-critical error or > 10% of the participants)	3	3	2
	HIGH (critical error or >30% participants)	1	1	1

The user acceptance test results were analyzed using the mean based on the 5-point Likert scale questionnaire score. Then, the overall mean of each construct was calculated and classified into three categories: Negative, Neutral, and Positive, which is based on the range of mean with values ranging from zero to five, as presented in Table II.

TABLE II. Range of Mean Value [30]

Category	Range of Mean
Negative	0.00–1.66
Neutral	1.67–3.33
Positive	3.34–5.00

The stress test is analyzed depending on which point the system will begin to show signs of failure when given increasing loads of requests. The vulnerability assessment's vulnerability scan results included an analysis of the vulnerabilities mapped with the Common Weakness Enumeration (CWE) [31]. The functionality test results are analyzed by comparing the expected output to the actual output. Mismatches (example: a High-Severity notification was expected, but a Medium-Severity notification was received) could mean errors and bugs that need to be fixed. Lastly, the cross-browser test produced a table containing data about which web browsers the system is incompatible/compatible with or has an unstable performance.

A. Functionality Testing

Functionality testing is an approach in software testing that verifies the system's expected behavior when performing specific functions. The test is broken into three parts; User, Administration, and Contact Tracing evaluated against the functional requirements/specifications. Each part consists of a group of functions; action is then performed to determine whether the system is functioning as expected. All tests conducted for functionality passed, as shown in Table III.

TABLE III. Summary of Functionality Testing Result

Functionality Test	Result
User Authentication	
Registration	Passed
Login	Passed
Contact Tracing	
Registration	Passed
Close Contact Identification	Passed
Contact Tracing Notification Generation	Passed
Infected Room Identification	Passed
Administration	
System Notification Generation	Passed
Movement Monitoring	Passed

B. Cross Browser Testing

Cross-browser testing [32] is a test that verifies the web application's compatibility with various browser combinations. The test featured popular browsers such as Google Chrome, Mozilla Firefox, Microsoft Edge, and Opera to test a series of functionalities that take various factors to evaluate against, depending on the functionality group.

All the web browsers tested and all the functionality available in the system are divided into sections or functional groups that are then evaluated against relevant factors. A checkmark indicates that a particular browser within a functionality group assessed against a specific factor behaves as expected and doesn't show any error or bugs, while a cross-check indicates the opposite. For example, while all the browser tests were successful, two were marked with a cross-check under the Mozilla Firefox web browser. Specifically, on the floor page under the sidebar "movements," the "time" and "date" selector would not display an interface to filter the time state, and the "date" selector for the user's birth date in the register page has a similar issue as well. The complete cross-browser testing result is shown in Table IV.

TABLE IV. CROSS-BROWSER TESTING RESULT

Cross-Browser Test	Browser Compatibility Remarks
Search Functionality	
Appearance and Layout	Compatible with all Browsers
Responsiveness	Compatible with all Browsers
Links and Redirects	Compatible with all Browsers
Navigation Menu	
Appearance and Layout	Compatible with all Browsers
Responsiveness	Compatible with all Browsers
Links and Redirects	Compatible with all Browsers
Contact Tracing Notifications	
Appearance and Layout	Compatible with all Browsers
Responsiveness	Compatible with all Browsers
Links and Redirects	Compatible with all Browsers
System Notification	
Appearance and Layout	Compatible with all Browsers
Responsiveness	Compatible with all Browsers
Links and Redirects	Compatible with all Browsers
Home Page	
Appearance and Layout	Compatible with all Browsers
Responsiveness	Compatible with all Browsers
Register Page	
Appearance and Layout	Not compatible with Mozilla Firefox
Responsiveness	Compatible with all Browsers
Form Functionality and Validation	Compatible with all Browsers
Login Page	
Appearance and Layout	Compatible with all Browsers
Responsiveness	Compatible with all Browsers
Form Functionality and Validation	Compatible with all Browsers
Floors Page (All)	
Appearance and Layout	Compatible with all Browsers
Responsiveness	Compatible with all Browsers
Form Functionality	Compatible with all Browsers
Floors Page (Specific)	
Appearance and Layout	Compatible with all Browsers
Responsiveness	Compatible with all Browsers
Form Functionality	Not compatible with Mozilla Firefox
Floor Plan Resizing	Compatible with all Browsers
Floor Plan Edit Overlays	Compatible with all Browsers
Card Page (All)	
Appearance and Layout	Compatible with all Browsers
Responsiveness	Compatible with all Browsers
Form Functionality	Compatible with all Browsers
Card Page (Create)	
Appearance and Layout	Compatible with all Browsers
Responsiveness	Compatible with all Browsers
Form Functionality	Compatible with all Browsers
Profile Page	
Appearance and Layout	Compatible with all Browsers
Responsiveness	Compatible with all Browsers
Edit Profile Page	
Appearance and Layout	Compatible with all Browsers
Responsiveness	Compatible with all Browsers
Form Functionality	Compatible with all Browsers

C. Stress Testing

Stress testing [33] is an approach in testing wherein the performance of the web application or system is measured and evaluated under heavy load conditions to measure its stability and reliability under extreme conditions. Apache Bench is a tool from the Apache organization designed to measure the performance of any HTTP web server. Apache Bench is configurable to allow users to specify values for the number of attempts reaching the web server, indicated by the "-n" option, and the number of concurrent connections displayed by the "-c" option. The test in the web application using Apache Bench was performed in seven successions. Each test corresponded with a higher parameter value (number of attempts and total concurrent connections) than the previous test. The test is finalized when the webserver processes 1,000 attempts and 1,000 concurrent connections in a single test.

Several stress tests were conducted on the Internet Information Services (IIS) webserver. The webserver that hosts KontaKard successfully handled 300 to 700 attempts and concurrent connections. A second test successfully handled 350 attempts and concurrent connections.

To test the prototype's performance, the time it took the scanner to indicate a response status (flash either a red/green color light via Light-Emitting Diode (LED) with a corresponding beep sound) after scanning a card was measured. Due to budget constraints, the study could produce only four scanners. The tests were performed in stages. Each stage has an incremented number of scanners than the previous test by 1. It is used to simultaneously send requests to the server to see if the time it takes for the scanner to provide both a visual and aural indication of the scan status will change. It's worth noting that the actual scan status displayed as the response speed was being tested did not matter (a successful scan was not necessary). Both successful and unsuccessful scan means that the request was sent from the scanner to the server. The scanner received a response from the server for it to know the status that it is supposed to display, which may vary and fail if either 1) the card is unregistered, 2) the card does not have an active status, or 3) the scanner is unregistered.

The time it takes for the scanner to respond to a card scan remains the same regardless of the number of scans done simultaneously with a maximum of four scanners. The processes of each scanner and card pair did not interfere with each other. The system determined if a card scan is invalid on a setup where the scanners were programmed to send Hypertext Transfer Protocol (HTTP) requests to the central server and await a response from it. Furthermore, the server was able to handle many concurrent requests. This means that the system effectively meets the efficiency requirements.

D. Usability Testing

Usability testing were conducted according to the designed roles of the users in the system. The summary of guests/employees' performance metrics based on the given set of tasks is shown in Table V. The results showed that Task 2 and Task 3 met the goal of a 100% completion rate. Task 3 received an error-free rate below 50% where the task was not completed efficiently. The errors did not impact the final output since it acquired a completion rate of 92%. Respondents were challenged but managed to complete the task, implying that the respondents learned how the feature works as they have completed the task.

The administrator's performance metrics based on the given set of tasks is shown in Table VI. The results showed that the tasks were 100% complete and error-free. In addition, the administrator had a positive experience with the system as he completed the tasks assigned. The 0 value under the error-free rate column aligned with the managing floors task was due to a non-critical error or issue that the administrator participant encountered. Only one administrator agreed to participate in the study, so these results were either fully completed or not.

TABLE V. SUMMARY OF TASKS OF GUESTS/EMPLOYEES

Task	Completion Rate (%)	Error-free Rate (%)	Time on Task Goal (minutes)	Time-on-Task Success Rate (%)
1.	Account Registration	96.43	60.71	3.00
2.	Using the card	100.00	96.43	2.00
3.	Viewing floor maps	92.86	46.43	4.00
4.	Receiving and viewing contact tracing notifications	100.00	57.14	1.00

TABLE VI. SUMMARY OF TASKS OF ADMINISTRATOR

Task	Completion Rate (%)	Error-free Rate (%)	Time on Task Goal (minutes)	Time-on-Task Success Rate (%)
1.	Authentication	100	100	1
2.	Receiving and viewing system notification	100	100	1
3.	Managing cards	100	100	2
4.	Managing floors	100	0	10
5.	Viewing reports	100	100	2
6.	Managing users	100	100	2

There is only one problem that the administrator participant experienced, as shown in Table VII during the test: "Floors control bar icons were not being recognized."

TABLE VII. USABILITY PROBLEM SUMMARY OF ADMINISTRATORS

Problem	Impact	Frequency	Classification
Floors control bar icons were not being recognized.	Moderate	100.00	Severity 2

The problems that the guest/employee participants experienced during the test are shown in Table VIII. The most frequent ones that occurred were the "Confusion in editing user profile due to the redirect pointing to the edit page again instead of the view page after submitting an edit" and "Floors control bar icons were not being recognized" problems. The problems with a severity of 1 were "Forgot password" and "Could not figure out how to change time state view." The result shows that these factors influenced the ability of users to complete tasks, which led to them having high impact and high severity. Apart from the users' problems during the tests, several comments, recommendations, and suggestions provided by the participants, as shown in Table IX, were not necessarily related to usability but were still deemed valuable.

TABLE VIII. USABILITY PROBLEMS SUMMARY OF GUESTS/EMPLOYEES

Problem	Impact	Frequency	Classification
Confusion in editing user profile due to the redirect pointing to the edit page instead of the view page after submitting an edit.	Moderate	35.71	Severity 2
Confusion as to which input fields were required during registration.	Low	3.57	Severity 4
Forgot password.	High	3.57	Severity 1
Confusion in notification dropdown not closing after clicking the bell icon again.	Low	7.14	Severity 4
Did not know that notifications only show up after refreshing the page.	Moderate	10.71	Severity 3
Thought the notifications were clickable.	Moderate	21.43	Severity 2
Did not like how the notification colors blended in.	Low	3.57	Severity 4
Could not figure out how to change the time state view.	High	3.57	Severity 1
Floors control bar icons were not being recognized.	Moderate	42.86	Severity 2
Confusion in movement controls *DateTime* selectors due to the option to select future dates.	Low	3.57	Severity 4
Could not figure out what the people present meant.	Moderate	3.57	Severity 3
Could not figure out how to select a room.	High	3.57	Severity 1
Did not understand the icons of virus and people on the rooms.	Moderate	3.57	Severity 3

TABLE IX. USER SUGGESTIONS AND FEEDBACK DURING USABILITY TEST

User Type	Suggestions/Feedbacks
Administrator	Restoration of deleted resources
	Contact number validation to filter out characters.
	Confirmation message before deleting resources.
	Import and export reports data.
	Notification to desktop or email.
	Graphical charts for the reports.
	More tooltips (for uniformity).
Health	Vaccination status in the profile.
	Contact information in the reports page for the close contacts.
Guests/Employees	Suggestions for the next possible steps for when a user receives a contact tracing notification.
	A step-by-step onscreen tutorial for first-time users.
	More content on the home page about contact tracing.

E. User Acceptance Testing

The USER acceptance Testing (UAT) used three different models, namely: the DeLone McLean IS Success Model, Unified Theory of Acceptance and Use of Technology (UTAUT) Model, and Task Technology Fit (TTF) model, integrated into one single model with two additional constructs. The model shall determine the association between the constructs and the user's intention in using the developed system, specifically: one exogenous variable, which is perceived user-technology-organization fit, and ten endogenous variables, which are performance expectancy (PE), effort expectancy (EE), social influence (SI), facilitating condition (FC), software quality (SWQ), information quality (IQ), service quality (SERQ), management support (MS), and information security expectancy (ISE). The User Acceptance Test (UAT) result, as displayed in Table X shows that users receive the system well. Scoring a high average of well over four on a 5-point Likert scale (where one equates to strongly disagree and five to strongly agree) on all the constructs used by the adopted model equates to a positive mean category that implies a high user acceptance rate.

TABLE X. SUMMARY OF USER ACCEPTANCE TESTING RESULT

Constructs in the User Acceptance of Healthcare technology Model	Impact	Frequency
Performance Expectancy (PE)	4.73	Positive
Effort Expectancy (EE)	4.77	Positive
Social Influence (SI)	4.63	Positive
Facilitating Condition (FC)	4.72	Positive
Software Quality (SWQ)	4.77	Positive
Service Quality (SERQ)	4.82	Positive
Information Quality (IQ)	4.82	Positive
Information Security Expectancy (ISE)	4.84	Positive
Management Support (MS)	4.84	Positive
Intention To Use (ITU)	4.77	Positive
Perceived User-Technology-Organization Fit (PUTOF)	4.79	Positive

F. Vulnerability Testing

In vulnerability assessment, OWASP ZAP was used. OWASP ZAP is an open-source web application vulnerability scanner. The results of testing showed ten alerts with varying priority levels: two medium, six low, and two informational priority alerts. Thus, the vulnerability scanner shall detect fulfilling security under a non-functional requirement that indicates no high risk or high priority vulnerability. The "Web browser data loading may be possible due to a Cross-Origin Resource Sharing (CORS) misconfiguration on the webserver." The summary of vulnerability testing results is shown in Table XI.

VI. CONCLUSION AND RECOMMENDATION

This research aimed to develop an RFID-based contactless smart card system to track people's movements within an establishment for purposes that

TABLE XI. SUMMARY OF VULNERABILITY TESTING RESULT

Risk Assessment	Results
MEDIUM	1. "X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks."
	2. "No Anti-CSRF Tokens were found in an HTML submission form,"
LOW	1. "A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a cross-site request." The SameSite attribute is an effective countermeasure to cross-site request forgery, cross-site script inclusion, and timing attacks".
	2. "The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content."
	3. "The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to" .
	4. The "Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server."
	5. "The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing".
	6. "The response appears to contain suspicious comments which may help an attacker".
INFORMATIONAL	"A timestamp was disclosed by the application/web server – Unix".

support security, activity inference, and an alternative contact tracing solution that supplements existing contact tracing solutions within the host establishment. To dynamically track people's movements within an establishment, RFID contactless smart card technology, combined with web application technology, was used to register users' locations and the date and time of their entry and exit to specific rooms in an establishment. This allowed for inferring activities and determining when people were present in a room, how long they were present, and who they were possible with.

This ability could also provide a secondary function of contact tracing by using contactless smart cards and scanners installed within an establishment to identify, monitor, and notify users who may have had close contact with a person diagnosed with COVID-19. Furthermore, the test results evaluated against the functional requirements show that the system behaved as intended when the corresponding action and validation were performed.

Lastly, the test results evaluated against non-functional requirements showed no report of known high risk or high priority vulnerabilities, thus ensuring that the system isn't vulnerable to critical and high-risk vulnerabilities. Further tests also showed a positive experience and high acceptance rate among the three types of users that the system caters to, thus proving that the system satisfied the user requirements and standards for a human movement-tracking system.

CONFLICT OF INTEREST

All authors declare that they have no conflicts of interest.

AUTHOR CONTRIBUTIONS

Ms. Samonte supervised the whole research development and took the lead in writing the manuscript. Mr. Medel did all the programming the system integration seamless. Mr. Odicta performed the integration of software and hardware components of the application. Ms. Santos assisted in the testing and writing of the final technical documentation of the project. All authors provided critical feedback and helped shape the research, analysis, and manuscript.

FUNDING

This research paper presentation and registration was funded by Mapua University.

REFERENCES

[1] P. R. Carnley and H. Kettani, "Identity and access management for the internet of things," *International Journal of Future Computer and Communication*, vol. 8, no. 4, pp. 129–133, 2019.

[2] C. Perra, A. Kumar, M. Losito, P. Pirino, M. Moradpour, and G. Gatto, "Monitoring indoor people presence in buildings using low-cost infrared sensor array in doorways," *Sensors*, vol. 21, no. 12, p. 4062, 2021.

[3] G. X. Liu, L. F. Shi, S. Chen, and Z. G. Wu, "Focusing matching localization method based on indoor magnetic map," *IEEE Sensors Journal*, vol. 20, no. 17, pp. 10012–10020, 2020.

[4] D. Rawat, V. Chaudhary, and R. Doku, "Blockchain technology: Emerging applications and use cases for secure and trustworthy smart systems," *Journal of Cybersecurity and Privacy*, vol. 1, no. 1, pp. 4–18, 2020.

[5] World Health Organization. (2020). Contact tracing in the context of COVID-19: Interim guidance, 1 February 2021. [Online]. Available: https://apps.who.int/iris/handle/10665/339128

[6] J. Amann, J. Sleigh, and E. Vayena, "Digital contact-tracing during the Covid-19 pandemic: An analysis of newspaper coverage in Germany, Austria, and Switzerland," *Plos One*, vol. 16, no. 2, e0246524, 2021.

[7] H. Y. Yuan and C. Blakemore, "The impact of contact tracing and testing on controlling COVID-19 outbreak without lockdown in Hong Kong: An observational study," *The Lancet Regional Health-Western Pacific*, vol. 20, 100374, 2022.

[8] K. Riemer, R. Ciriello, S. Peter, and D. Schlagwein, "Digital contact-tracing adoption in the COVID-19 pandemic: IT governance for collective action at the societal level," *European Journal of Information Systems*, vol. 29, no. 6, pp. 731–745, 2020.

[9] M. Klenk and H. Duijf, "Ethics of digital contact tracing and COVID-19: Who is (not) free to go?" *Ethics and Information Technology*, vol. 23, no. 1, pp. 69–77, 2021.

[10] R. Chandramouli, "Infrastructure system design methodology for smart cards deployment," in *Proc. the IADIS International Conference on Information Systems 2008*, 2008, pp. 115–122.

[11] D. A. Lindeman, K. K. Kim, C. Gladstone, and E. C. Apesoa-Varano, "Technology and caregiving: Emerging interventions and directions for research," *The Gerontologist*, vol, 60, pp. S41–S49, 2020.

[12] A. Polenta, P. Rignanese, P. Sernani, N. Falcionelli, D. N. Mekuria, S. Tomassini, and A. F Dragoni, "An internet of things approach to contact tracing — The Bubblebox system," *Information*, vol. 11, no. 7, p. 347, 2020.

[13] M. T. Rahman, R. T. Khan, M. R. Khandaker, M. Sellathurai, and M. S. A. Salan, "An automated contact tracing approach for controlling COVID-19 spread based on geolocation data from mobile cellular networks," *IEEE Access*, vol. 8, pp. 213554–213565, 2020.

[14] MF1S70YYX_V1. (2017). MIFARE classic EV1 4K-mainstream contactless smart card IC for fast and easy solution development. [Online]. Available: https://www.nxp.com/docs/en/data-sheet/MF1S70YYX_V1.pdf

[15] Department of Health, Republic of the Philippines. (2020). Updated guidelines on contact tracing of close contacts of confirmed Coronavirus Disease (COVID-19) cases. [Online]. Available: https://doh.gov.ph/sites/default/files/health-update/dm2020-0189.pdf

[16] Department of Health, Republic of the Philippines. (2020). Omnibus interim guidelines on prevention, detection, isolation treatment, and reintegration strategies for COVID-19. [Online]. Available: https://upd.edu.ph/wp-content/uploads/2022/01/DOH-Guidelines.pdf

[17] J. Ahn, F. Campos, M. Hays, and D. DiGiacomo, "Designing in context: Reaching beyond usability in learning analytics dashboard design," *Journal of Learning Analytics*, vol. 6, no. 2, pp. 70–85, 2019.

[18] COVID-19 Response Protocol. (2020). [Online]. Available: https://www.uidaho.edu/-/media/UIdaho-Responsive/Files/health-clinic/covid-19/reopening-plans/covid-response-protocols.pdf

[19] Department of Health, Republic of the Philippines. (2020). Workplace handbook on COVID-19 management and prevention. https://philguarantee.gov.ph/wp-content/uploads/2021/10/Workplace-Handbook-COVID-Prevention.pdf

[20] Department of Health, Republic of the Philippines. (2020). Case investigation form Coronavirus Disease (COVID-19) version 8. [Online]. Available: https://batmc.doh.gov.ph/images/2021/eCIF_version_8_Fillable_-_Molecular_Diagnostics_Laboratory.pdf

[21] The Progressive JavaScript Framework (Vue.js). [Online]. Available: https://vuejs.org/

[22] MySQL. [Online]. Available: https://www.mysql.com/

[23] Python. [Online]. Available: https://www.python.org/

[24] B. Rahimi, H. Nadri, H. L. Afshar, and T. Timpka, "A systematic review of the technology acceptance model in health informatics," *Applied Clinical Informatics*, vol. 9, no. 3, pp. 604–634, 2018.

[25] H. Taherdoost, "A review of technology acceptance and adoption models and theories," *Procedia Manufacturing*, vol. 22, pp. 960–967, 2018.
[26] S. B. Ali, J. Romero, K. Morrison, B. Hafeez, and J. S. Ancker, "Focus section health IT usability: Applying a task-technology fit model to adapt an electronic patient portal for patient work," *Applied Clinical Informatics*, vol. 9, no. 1, pp. 174–184, 2018.
[27] B. Mburano and W. Si, "Evaluation of web vulnerability scanners based on OWASP benchmark," in *Proc. 26th International Conference on Systems Engineering (ICSEng 2018)*, 2018, pp. 1–6.
[28] D. P. Drljaca and B. Latinovic, "Using TELOS for the planning of the information system audit," *Materials Science and Engineering*, vol. 294, no. 1, 012022, 2018.
[29] Usability.gov. Usability test plan template. [Online]. Available: https://www.usability.gov/how-to-and-tools/resources/templates/usability-test-plan-template.html
[30] M. N. Osman, K. A. Sedek, M. Maghribi, and N. H. M. Faisal, "ANotify: A fingerprint biometric-based and attendance web-based management system with SMs notification for industrial sector," *Journal of Computing Research and Innovation*, vol. 3, no. 1, pp. 36–45, 2018.
[31] K. Kanakogi, H. Washizaki, Y. Fukazawa, S. Ogata, T. Okubo, T. Kato, H. Kanuka, A. Hazeyama, and N. Yoshioka, "Tracing CAPEC attack patterns from CVE vulnerability information using natural language processing technique," in *Proc. the 54th Hawaii International Conference on System Sciences*, 2021, pp. 6996–7004.
[32] L. N. Sabaren, M. A. Mascheroni, C. L. Greiner, and E. Irrazábal, "A systematic literature review in cross-browser testing," *Journal of Computer Science & Technology*, vol. 18, no. 2, pp. 1–3, 2018.
[33] F. Costa, S. Genovesi, M. Borgese, A. Michel, F. A. Dicandia, and G. Manara, "A review of RFID sensors, the new frontier of internet of things," *Sensors*, vol. 21, no. 9, 3138, 2021. https://doi.org/10.3390/s21093138

Mary Jane Samonte has a double bachelor's degree in computer education and information technology. She also finished two graduate degrees in information technology and computer science, with one doctoral. She has more than twenty years teaching experience in tertiary level. She has a wide range of research interests that are centered around educational technologies, gamification, mobile and ubiquitous learning, digital game-based learning, artificial intelligence in education, e-health, assistive technology, natural language processing, green computing and data analytics-based studies.

Darwin A. Medel graduated as Magna cum laude with a silver medal in the bachelor of science degree in information technology program of the School of Information Technology at Mapúa University—Makati. Automation and the development of new technologies are what he is most passionate and curious about. Presently, he is working as an internal applications developer for Sophos, a company that develops software and hardware cyber security products.

Joshua Millard N. Odicta graduated as cum laude undertaking a bachelor of science in information technology at Mapua University. He is now working as a SOC analyst at Red Rock IT Security Inc.

Ma. Zhenadoah Leen T. Santos graduated as Magna cum laude from Mapúa University with a bachelor of science degree in information technology and specialized in cyber security. Her interests include application and web development, network security and management, applied cryptography, and digital forensics. She is currently a UI/UX Designer in JuanTax, the Philippines' first Bureau of Internal Revenue (BIR) accredited tax solution platform.