International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 1 (2018) pp. 749-760

Detecting Unauthorized RFID Tag Carrier for Secure Access Control to a Smart Building

Ahmed Raad Al-Sudani[a], Wanlei Zhou[b], Bo Liu[c], Ahmed Almansoori[d] and Mengmeng Yang[e]

[abde] *School of Information Technology, Deakin University, Burwood, 3125, Australia.*

[c] *Department of engineering, La Trobe University, Melbourne, 3086, Australia.*

[a]*Orcid: : 0000-0002-2921-9124*

Abstract

The human race has evolved from apelike ancestor to the present state. Technology innovations are continuously promoting civilization in the world. Nevertheless, human race suffers from the menace of anti-social elements. Protecting people and their properties from terrorists is now an indispensable agenda for modern society. Towards this end, technology has been playing a big role. With the emergence of IoT around the corner, the Radio Frequency Identification (RFID) is being used to identify objects uniquely and tracking them by associating RFID tag to such objects. By integrating physical and digital worlds, it is possible to safeguard interests of stakeholders in any given outfit. In the existing systems, tag collision and inefficient matching are the two issues in the authentication process. To overcome this problem, in this paper, we considered a smart building which is to be protected from unauthorized human access. People with valid RFID tag and valid proof of biometric identification can only enter into the smart building. To realize this secure access control to a smart building, we proposed a framework that has underlying mechanisms to detect unauthorized RFID tag carrier for secure access control to a smart building. Two algorithms namely Adaptive Collision free Tag Identification Algorithm (ACTIA) and Image Matching Algorithm (IMA) with SURF feature-point and DAISY descriptor to implement the framework are proposed. We built a model application to demonstrate proof of the concept. In addition, considering the privacy problem in RFID, we insert a hardware module which has a Trusted Platform Module (TPM) chip into the RFID reader. Our experimental results revealed that the proposed system is capable of detecting people who do not have registered RFID along with the image of the person and raise appropriate alarm to alert authority concerned.

Keywords: RFID, smart building, secure access control, image matching, privacy preserving

INTRODUCTION

RFID technology uses the electromagnetic field to identify and track tags associated with objects. This way, RFID enables physical objects also to participate in computing and get integrated with the digital world. Tags are also known as labels used to have a unique identification. A tag holds electronically saved information about the object with which it is associated. RFID tags are of three kinds namely passive, active and semi-passive. Passive RFID tags can obtain energy from the interrogating radio waves from nearby RFID reader while active RFID tags are equipped with local power source and support recognition from hundreds of meters. Nevertheless, active RFID suffers from lifetime issues. RFID is the enabling technology of Internet of Things (IoT). It plays a key role in the security case study of this paper that is smart building. Passive tags are cheaper while the active tags are costly. Semi-passive RFID tags do have battery power and also the capability to exploit the energy of radio waves of RFID reader. Thus semi-passive is considered a suitable candidate which is more reliable and covers more range when used with smart building case study. It has long read and write capabilities. When compared with the barcode which is attached to objects for identification, RFID is the best technology which does not suffer from a line of sight problem as well. Many real world applications are using RFID technology as found in the literature. It is used to patient identification and tracking in healthcare units (1, 2). RFID is widely used in supply chain management applications(3), animal data recording systems (4), lean manufacturing (5), public transport systems (6), inventory management systems(7), precision agriculture applications (8), and for secure authentication(9-13). However, in many RFID based authentication systems, tag collision and inefficient image matching are the two problems identified. In addition, the privacy problem was not considered. The main privacy concern with RFID are the tracking of people and their locations and gain the people's habit, which can be used to infer users' sensitive information or even cause security problems, such as identity theft and robbery. In this paper, RFID is used to have smart building case study and mechanisms to overcome the problems. RFID implementations in the real world do contribute to privacy issues.

We proposed a framework for RFID based secure access control of humans to a smart building. Semi-passive RFID tags are considered for the realization of the case where humans are registered with the system with RFID tag and biometric image. Once a person is registered with the smart building digital infrastructure, the person is subjected to secure access control and authentication every time the person enters into the premises of the smart building.

We proposed two algorithms for secure access control. The first algorithm is to identify RFID tag and match it with the database. It is adaptive and collision free. The second algorithm is for matching the image registered in the database. We used SURF feature-point and DAISY descriptor for highly reliable and faster matching of images for two-fold authentication

which involves both tag verification and image matching. We built a model application using Python language. The application is realized the framework proposed with underlying algorithms to demonstrate proof of the concept laboratory experiments.

The remainder of the paper is structured as follows. Section 2 reviews literature pertaining to RFID technology, its evolution, and its applications in various diversified domains in the real world. Section 3 presents the proposed methodology for secure access control to a smart home based on RFID technology. It throws light into the algorithms proposed to verify RFID tags and live to match of images for secure digital authentication. Section 4 provides model implementation details. Section 5 presents experimental results while section 6 concludes the findings in this research paper besides providing directions for possible future work.

RELATED WORKS

This section provides the review of literature pertaining to RFID technology and its adoption, application of RFID and security in RFID enabled systems.

A. RFID Technology and Its Adoption

As explored in (1)RFID adoption is influenced by social issues competitive pressure and technology competence. The determinants that influenced the promotion of RFID in the healthcare sector include ease of use, usefulness, advantage, government policy, management support and security concerns (14). Adhiarna et al. (15) proposed a framework for RFID adoption that gives importance to scale, stage and scope. The scale includes organization, industry, and country. Stage contains preliminary, intermediate and mature while scope includes strategy, technology, organization, people, and environment. Vlachos (16) explored impact of RFID practices where systems like inventory management in terms of performance up to 45.6%. Many case studies of inventory management systems realized by RFID technology are explored in (17). The utility of RFID in inventory management as a strategic tool is studied by Alfaro et al. (18). Similar kind of research was carried out by Mokshin and Hamidi (7). Shaik et al. (3) found that RFID has its increasing impact on SCM, Internal SCM, Supplier Relationship Management (SRM) and CRM. RFID with WLAN is explored in SCM (19). Similar kind of research was made in (20). Service Oriented Architecture (SOA) played a vital role in RFID integration (21). RFID specific knowledge management systems are explored in (22). RFID for a knowledge based economy (KBE) is explored in (23)in the context of high-tech clusters. RFID implementation in SCM showed critical management issues. They are related to information management and processes management (24). The positive feasibility of RFID survivability is established in (25). Bendavid et al. (26)opined that organizations in the real world are pressurized to have better results with RFID technology and innovation in rendering services for internal and external stakeholders. Ferrer and Geraldo (27) investigated on the right usage of RFID and found that different applications need a different approach in using RFID. For instance, ATM cash transfer scenario needs active RFID while highway and city toll collection should have passive RFID. Different cases identified for RFID usage include mine worker identification, student location, theme park visitor location, Meals Ready to Eat (MRE) control, refrigerator cargo control, fashion boutique management, speciality container identification, hospital patient identification, container tracking in oceans, healthcare laboratories, automobile distribution yard, and container yard management to mention few. As explored in (28) the role of integration technology is growing due to distributed applications in the real world and RFID plays a vital role in this scenario. Quetta and Pigni (29) explored vertical supply chain and RFID adoption in such environment. They considered many factors in their investigation including technology maturity, competitive pressure, industry, emulation effect, normative, incentives, supervisor, and privacy. They found that organizational readiness plays important role in RFID technology adoption.

B. RFID Applications

Azevedo et al. (30) employed RFID technology to Supply Chain Management related to fashion (FSCM). They used RFID for leveraging logistics functionality, product quality, tracking or products and making the FSCM system more responsive. The problem they encountered is interoperability. Similarly, Chan and Chong (31) studied the usage of RFID in mobile SM. With respect to supply chains, trust acts as a catalyst for integration RFID (32). Wamba et al. (2) explored different healthcare applications that are RFID enabled. Asset management and remote healthcare are two important observations enabled by RFID. Beheshti et al. (33) studied the implementation of ERP with RFID technology found that it plays a vital role in future for successful ERPs. RFID is adopted to have fully automated hospital information system. In such systems, the factors to be prioritized include technology competence, vendor support, security, and infrastructure and management support (34). RFID is found in many healthcare applications. Yao et al. (35)found that RFID integration with healthcare systems provided advantages like increasing Quality of Service (QoS), better tracking of equipment and improvement in clinical practices. Huang et al. (11) studied RFID technology for building a framework known as Mobi-Cloud. Samad et al. (4) proposed RFID based animal data recording mechanism with high-credibility. They opined that RFID technology adaptation becomes easier when the implementation is done in collaboration with other business in the similar chain. Lewis et al. (36) studied the impact of RFID usage in improving process performance in healthcare domain. They found that RFID has more benefits when compared with its counterpart that is a barcode. Terzian et al. (37)focussed on middleware needed for integration of systems with RFID. They proposed a middleware known as UbiRoad for context-aware smart road environments as part of intelligent transportation systems.

C. RFID for Security

Security risks in RFID systems are explored in (38). The risks include entity security risk caused by interference, theft, flaws in protocols and Point of Sale (POS) security risk caused in authentication module, and Business Information System (BIS) security risk caused by storage and audit mechanisms. Baldini et al. (9) studied RFID for securing disaster supply chains. They found the utility of cryptography used with RFID in order to achieve the desired security. They found that emergency crisis response systems in future can be improved with RFID. Prasad and Rajesh (39) proposed an architecture for real time patient management in healthcare domain using RFID. RFID is used to identify medical equipment uniquely. Kim (12)focused on security with RFID in terms authentication between mobile agent and RFID tag in Healthcare system. Different attacks such as eavesdropping, traffic analysis, message modification, replay and Denial of Service (DoS) are studied in the presence of sensor network, database agent, network agent, wireless network, mobile agent, and sensor network. Tampering RFID can have its risks and implementations and provided two kinds of prevention against tampering known as tamper-evidence and tamper-evidence. In the same fashion, the risks of tampering are damage and alteration. Huang et al. (11)proposed MobiCloud, a cloud based framework, for mobile computing and communication that are cloud-based. In this context, the significance of RFID is investigated with respect to have secure communications. In the inter-people scenario, RFID is used for accurate identification of humans. Feldhofer et al. (10)focused on studying semi-passive RFID tags and their ability to withstand security threats. They built demo tag architecture with architecture and verified RFID standards against security threats. Mubarak et al. (40) explored a Trusted Platform Module (TPM) for mutual attestation using RFID trusted protocol. For encryption of data, they used AES standard. Thus they built trusted computing technology based on RFID for integrity verification. Kurkovsky et al. (13)focused on continuous RFID-enabled authentication and studied privacy implications. They found that RFID usage continuously enables secure authentication. Interestingly, Monahan and Fisher (41)studied ethical and social risks of adopting RFID devices that are implantable. They found that the adoption of implantable RFID devices can cause issues like patient misunderstand ability, reduction of trust, and unfair prioritization of patients. They also found that RFID implants may result in social inequalities in obtaining services related to healthcare. Rethinking RFID in terms of its usage and interaction with other systems is investigated in (6) as the RFID tags also carry security risks with them. As the technology is invisible to RFID users and it is not under control of users, it may cause security threats and privacy concerns. They studied reader awareness which provides valuable feedback to users. Peng and Bao (42) proposed a RFID ticketing system with security. It is used for public transport. They proposed two protocols that comply with three principles. They principles include usage of strong cryptographic primitive, database support, and simple billing system. On the other hand, Li and Huang (43) focused on trust based security management in RFID based systems. They found many challenges in trust management. They include lack of centralized authority, heterogeneous models of trust, multiple levels of trust, diverse mobility models, high dynamics in trust groups, privacy concern, and open computing environment. Zero Knowledge Authentication Protocol (ZKAP) is explored in (44) based on alternative mode with respect to RFID systems. It was found to resist attacks such as forgery, a man in the middle, replay and tracking. Many techniques in the literature are found to secure RFID systems. However, a comprehensive approach with case study is still desired. In this paper, we proposed a RFID based security system for a smart building which ensures two-fold authentication service with a high true positive rate.

PROPOSED METHODOLOGY FOR DETECTING UNAUTHORIZED RFID TAG CARRIER

Our methodology is based on the case study considered in which is a smart building containing RFID based secure access control. The system is made up of different components. They are RFID tag, RFID reader, camera, GSM modem, micro controller, storage for RFID registrations, server, door locks and alarms. RFID tag used in the system is semi-passive RFID which has battery power and it can also use power from radio waves emitted by an antenna associated with RFID reader. RFID reader is the device which can read RFID tags from objects to which they are associated. The camera is used to capture the live image of the human who needs to get authenticated by the proposed system. The camera is installed in the entrance of smart home from which it takes images of visitors and sends to the server for authentication. The server is the application runs on a machine which has the capability to execute algorithms and authenticate RFID tags and humans who carry the tags. The micro controller is the component used to control the flow of execution. Storage is needed to store registrations with RFID and human images. Door locks are the devices that are used to lock or unlock doors. Alarms are used to notify violations to authorized people. The broad outline of the proposed system is as shown in Figure 1.

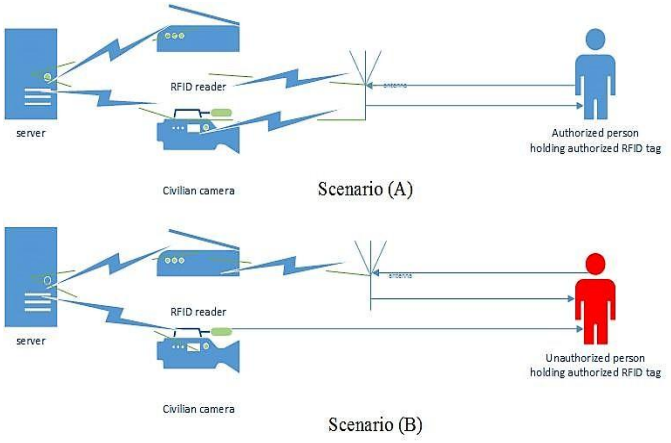

Figure 1: Broad overview of the proposed system

RFID reader and camera are connected to the server. RFID readers are associated with the corresponding antenna. Two scenarios are illustrated. The first scenario is the authorized person holding authorized RFID tag. The second scenario is the

unauthorized person holding authorized RFID tag. There is a two-fold process for secure access control to humans to allow into a smart building. The first process is to read RFID tag and verify it for its authenticity. Once RFID tag is verified and it is valid persons tag, the system performs image matching based on the image captured by the camera. The image matching is made to know whether the person is really a registered person. Though the person carried valid RFID tag, failure in image matching results in the failure of the authentication process. Thus two-fold verification process is considered highly effective, unlike its single RFID tag based authentication system. The system operation is as illustrated in Figure 2.

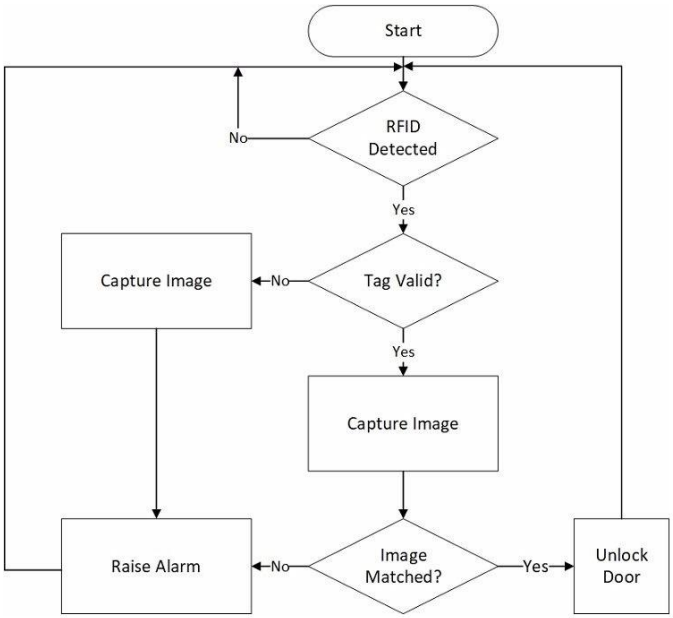

Figure 2: RFID based two-fold authentication

A. Adaptive Collision-free Tag Identification Algorithm (ACTIA)

This algorithm considers tag collision which is an important consideration in the scenarios where there are two possibilities. When multiple RFID readers co-exist in given area and interfere with other readers while reading RFID tag of a single object it is known as reader collision. On the other hand, tag collision occurs when multiple tags are concurrently conveying to the same reader. In other words, tag collision is the collision due to signals of multiple tags reaching tag reader simultaneously. We assume that this paper deals with the second scenario that is tag collision. Both reader collision and tag collision scenarios are illustrated in Figure 3.

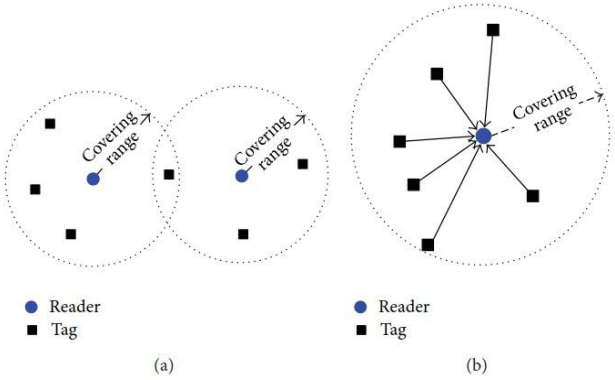

Figure 3: (a) Illustrates reader collision, (b) a tag collision in RFID based authentication (45)

The tag collision is the possibility assumed in the smart building scenario. When multiple people carrying RFID concurrently, the system needs to authenticate them without causing the collision. This algorithm is the meant for tag verification as part of the proposed two-fold authentication security. The algorithm takes tag information of multiple tags associated with human objects as input and checks in the storage of the system in the server. As soon as RFID reader reads RFID tag, this algorithm is executed by the server to know whether the tag is valid or not. If the tag is valid, the camera captures the image of the person and moves to image matching process. If not, the alarm is raised to notify the violation. This algorithm is crucial for the completion of two-fold authentication. Once it is successful, it moves to the image matching algorithm which makes use of SURF feature-point and DAISY descriptor for quick and accurate matching of images.

B. Image Matching Algorithm (IMA)

This algorithm is presented here in the form of the flow chart. The flowchart presented in Figure 4 shows the step by step procedure that starts from the bottom and moves on to top until image matching takes place. The image matching algorithm is inspired by the work explored in (46).

Algorithm: Adaptive Collision-free Tag Identification Algorithm

Inputs : RFID tag information *tinfo* of multiple tags *T*

Output : Image of visitor *img* and move to image matching/ image of the visitor *img* and

notification of violation *alarm*

1: Initialize *TD* to hold tag info database

2: Initialize *found* to hold false

3: for stepN=1 to size(*T*) do

4: for i=1 to size(*TD*) do

5: if *tinfo=TD[i]* then
6: *found* = true
7: break;
8: end if
9: end for
10: if *found*=true then
11: RFID tag is valid
12: capture image *img* of visitor
13: move to image matching process
14: else
15: capture image *img* of visitor
16: notify violation *alarm*
17: end if
18: end for

Algorithm 1: Adaptive Collision-free Tag Identification Algorithm

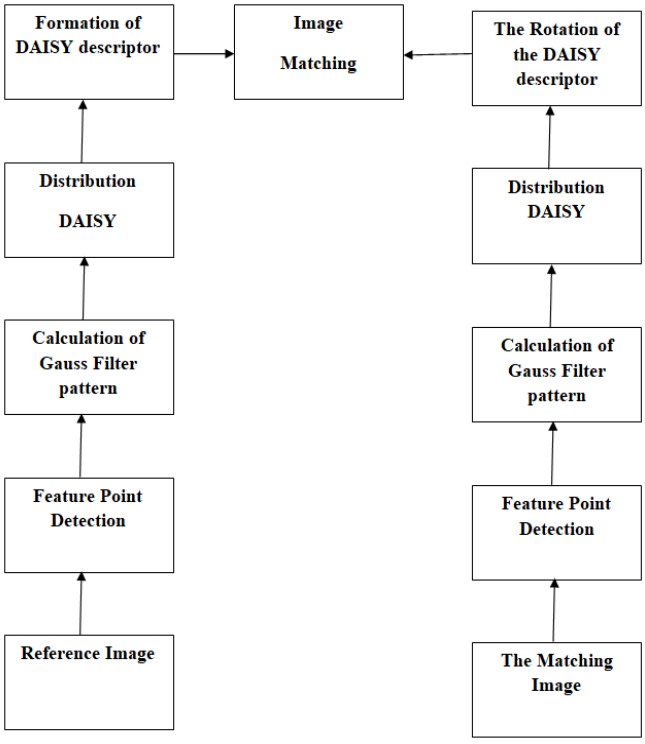

Figure 4: Image matching algorithm (IMA)

After successful tag verification, the captured image by the camera is sent to the server. Then the server program takes the matching image and subjects it to feature point detection. Towards this end, Hessian matrix of the matching image is computed as in Eq. 1.

$$H(X,\sigma) = \begin{bmatrix} L_{xx}\ (X,\sigma) & L_{xy}\ (X,\sigma) \\ L_{xy}\ (X,\sigma) & L_{yy}\ (X,\sigma) \end{bmatrix} \quad (1)$$

The convolution of the image is denoted as L. It is nothing but the second derivative of the Gaussian. Determinant according to SIFT algorithm which is meant for speeding up the matching process is as in Eq. 2.

$$\det(H) = \frac{\partial^2 f}{\partial^2 x^2}\ \frac{\partial^2 f}{\partial^2 y^2}\ -\left(\frac{\partial^2 f}{\partial^2 x \partial y}\right) \quad (2)$$

After choosing feature points, Gaussian filter pattern is captured. After this, DAISY descriptor is obtained from given image. This process is shown in Eq. 3.

$$\bar{x} = \frac{\partial^2 H^{-1}}{\partial^2 x}\ \frac{\partial H}{\partial x} \quad (3)$$

Once DAISY descriptor is in place, sample and representative points are computed as shown in Eq. 4 and Eq. 5.

$$Dx(X_i) = I(X_i^1) - I(X_i^5) \quad (4)$$

$$Dy(X_i) = I(X_i^3) - I(X_i^7) \quad (5)$$

The same process is computed to form DAISY descriptor for the reference image in the database. The two DAISY descriptors are matched. The result of matching is either positive or negative. In the case of the correct match, the two-fold authentication process is completed and the person is allowed into the building by unlocking doors. If the matching fails, the system raises alarm to notify violation to person concerned.

Algorithm: Image Matching Algorithm (IMA)

Inputs : Reference Images Database *RDB* and matching image *img*

Outputs : Violation notification alarm or unlock door

1: Initialize *IDB* to hold image database *RDB*
2: Initialize *found* to hold false
3: for i=1 to size(*IDB*) do
4: if DAISY(*img*)=DAISY(*IDB[i]*) then //use Eq. 1, Eq. 2, Eq. 3, Eq. 4 and Eq. 5
5: *found* = true
6: break;
7: end if
8: end for
9: if *found*=true then
10: Image matched
11: Authentication successful
12: Unlock door
13: else
14: Authentication failed
15: notify violation *alarm*
16: end if

Algorithm 2: Image matching algorithm

The algorithm is used to have image matching procedure based on the DAISY descriptor of the query image and reference images in database exact and efficient matching is made with faster convergence. In order make experiments we collected image dataset from (47). In fact, it is the dataset of faces provided by Cambridge University Computer Laboratory in conjunction with AT&T Laboratories. The images are of 40 subjects. Each subject has 10 images captured at different times, varying facial expressions and lighting conditions. They are in.PGM format with size 92x112 pixels and 256 grey levels per pixel.

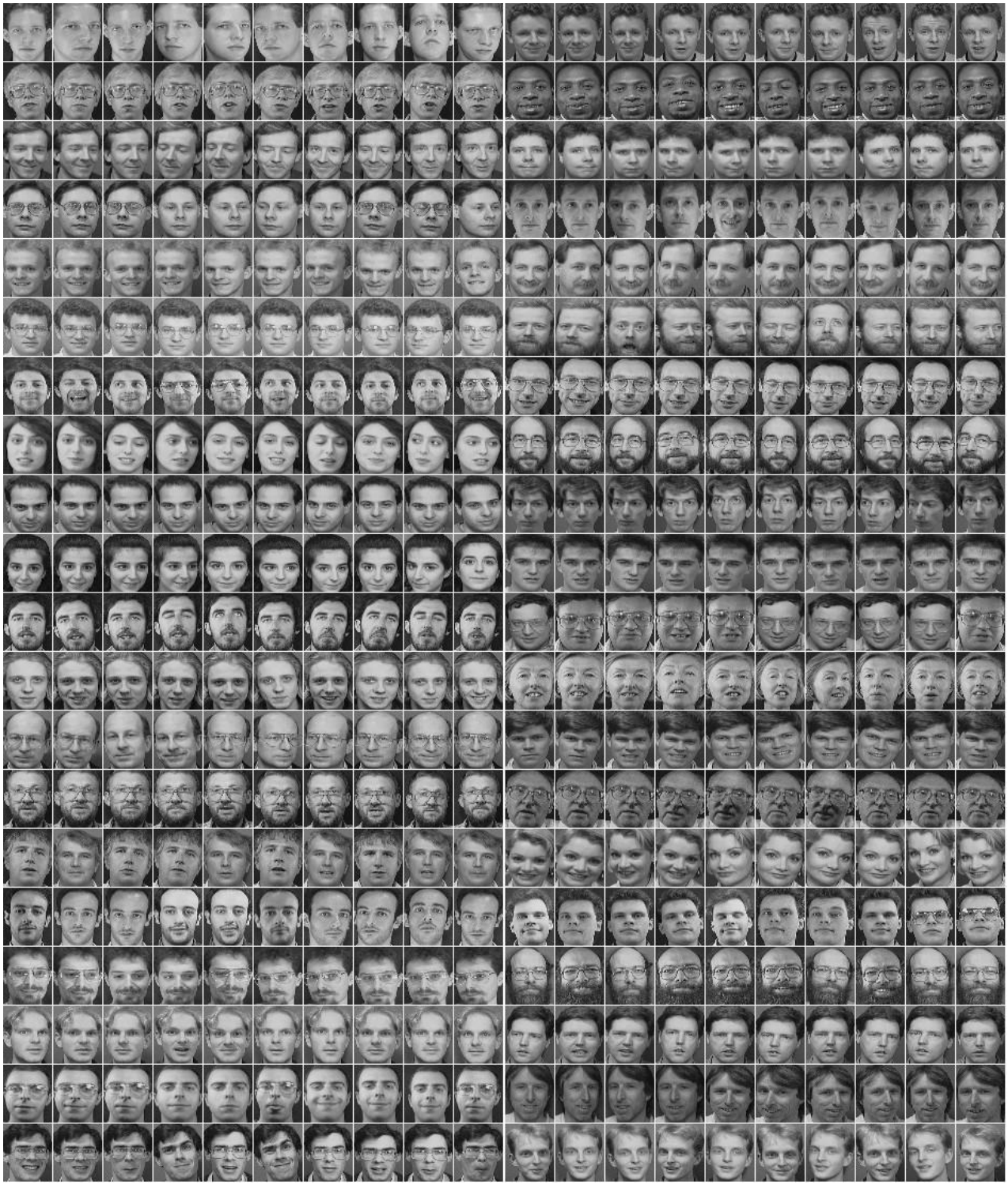

Figure 5: An excerpt from face image database (47).

Figure 5. As can be observed, the set of face images of each subject is captured with different lighting conditions, different times and facial expressions. The rationale behind this is to be close with real time scenarios encountered with the smart building case study chosen in this paper.

C. Privacy consideration

Numerous protocols have been proposed to protect the user's privacy in RFID system under different situations, such as zero knowledge based protocols (48)and double challenge response protocol (49). While to protect the user's privacy in the proposed system, we adopt the method proposed by Molnar et al. (50), which is proved simple but effective. The method works by inserting a Trusted Platform Module chip to the RFID reader. Such that even if a malicious user compromises the reader, he cannot break into the TPM. The user's personal information is protected.

EXPERIMENTAL RESULTS

The case study considered is a smart building which is protected from unauthorized access using RFID based security mechanism as illustrated in Figure 1 and based on the methodology described in section 3. Though the scenario is real time, to avoid the cost of equipment, the two algorithms proposed in this paper namely TIA and IMA are evaluated with a set of laboratory experiments for proof of the concept. A model application is built using Python language and SQLite database engine is used to manage RFID tags and AT and T image dataset. A computer with Inter Core i5-421OU CPU with a 1.70GHz process, 4.0 GB RAM running Windows 10 64-bit OS is used for experiments. As far as tag identification is concerned, the proposed algorithm named TIA is executed and results are captured. If the TIA provides a positive result, then the execution proceeds to IMA. Since IMA involves biometric identification of humans uniquely across the globe, IMA results are captured and compared with other matching algorithms known as SIFT and SURF. The IMA is evaluated with standard AT&T containing 10 face images on 40 subjects. Experiments are made for all 10 images of each subject and average performance is recorded in terms of time taken in seconds and accuracy of matching. Matching is performed as per the IMA algorithm presented in Figure 4. As a set of 10 face images of a specific subject do have the difference in terms of lighting condition, facial expression and timing, each image showed different performance. Therefore, the average performance of each subject is recorded. Since SIFT and SURF are two popular methods for image matching, IMA which makes use of DAISY descriptor is compared with those algorithms. Table 1 provides average accuracy % of each algorithm for 10 face images of each subject. It also has average accuracy % of all five subjects of AT&T face image database. In the same fashion, Table 2 has observations related to execution time taken for each algorithm with the same database. As per the average accuracy, IMA showed 87.26 for S1 which is far better than that of SIFT and SURF. For the same image, SFIT and SURF showed 59.01 and 71.2 % of matching accuracy respectively. The performance of algorithms differs for each image pertaining to given subject for the reason aforementioned. The face image S2 showed least matching performance for all the algorithms. In this case, SIFT could perform better as it has robustness against rotational invariance. This is the case with other images like S3 and S4 as well. The highest accuracy is 87.26 % shown by the proposed algorithm, IMA, in this paper. Figure 6 visualizes the dynamics of image matching performance of the three algorithms.

Table 1: Average accuracy (%) of matching with different subjects of AT&T dataset

Algorithms	Average Accuracy (%)					
	S1	S2	S3	S4	S5	Average
SIFT	59.01	35.78	72.5	82.1	85.15	66.908
SURF	71.2	30.89	68.25	70.45	86.71	65.5
IMA	87.26	35.12	71.48	79.34	86.54	71.948

Table 2: Average execution time for matching with different subjects of AT&T dataset

Algorithms	Average Execution Time (seconds)					
	S1	S2	S3	S4	S5	Average
SIFT	60.45	83.23	143.87	49.62	70.91	81.616
SURF	6.22	8.59	15.99	5.49	7.14	8.686
IMA	9.85	11.95	17.84	9.22	9.98	11.768

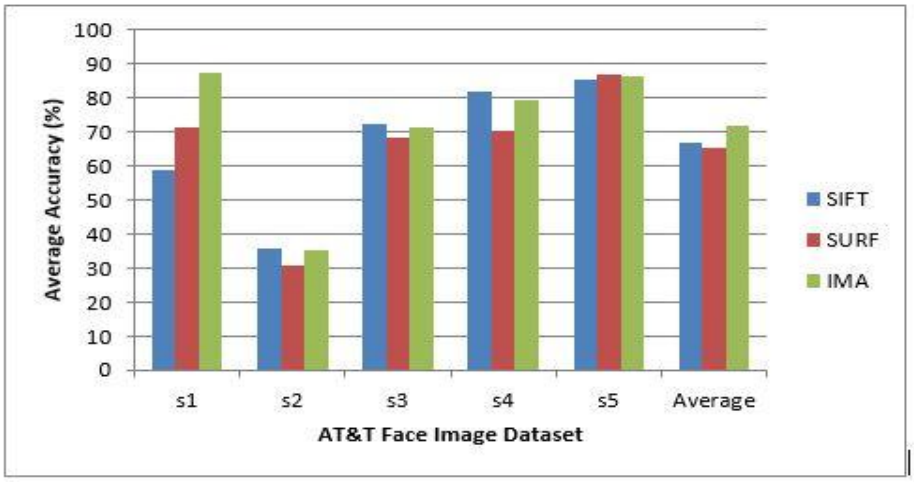

Figure 6: Image matching performance comparison

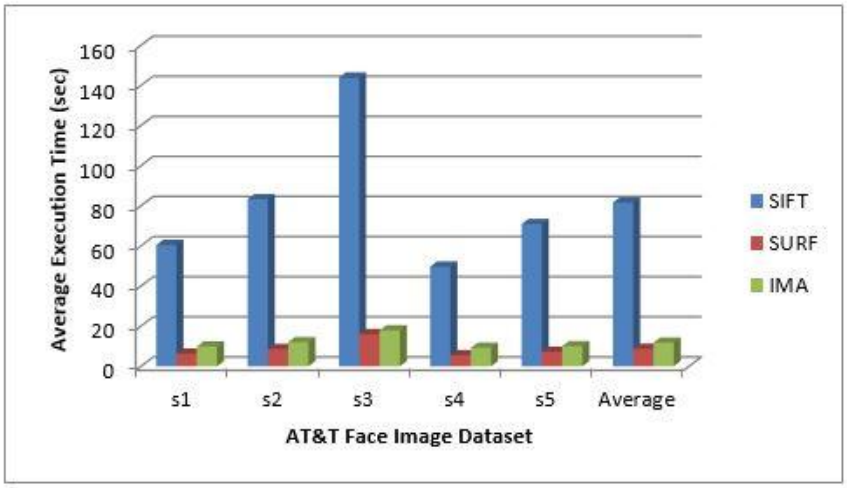

Figure 7: Execution time comparison IMA with other algorithms

Highest average accuracy is recorded with subject 1 faces. It is for the algorithm IMA. With respect to subject 2, subject 3 and subject 4 SIFT showed better performance over SURF and IMA. With subject 5 SURF showed better performance than other two algorithms. For all the subjects considered in the experiments, the SURF algorithm showed least matching accuracy except in the case of subject 5 and subject 1. SIFT showed the least performance with subject 1. The last data series shows the average matching performance of the three algorithms for all subjects considered. The proposed algorithm IMA showed the highest performance with 71.948 % matching accuracy while the SURF showed the least performance with 65.5 % accuracy. Nevertheless, SIFT showed 66.908 % of matching accuracy which is better than that of SURF. The execution time is observed in seconds. The time taken for each face image in a given subject of AT&T face image dataset is recorded. Then the average of all 10 images of each subject is computed and the results are presented for five subjects. Then the average of all subjects is also provided in the last column of Table 2. The results reveal that SURF has superior performance over other two algorithms in all subjects. The rationale behind this is that SURF has mechanisms that make it computationally effective. However, it showed poor performance related to matching accuracy. SIFT showed poor performance for all subjects in terms of execution time. The rationale behind this is that SIFT descriptor is very complex and building it is time-consuming. IMA shows superior performance over SIFT but performs poorly when compared with SURF. There is considerable complexity involved in DAISY descriptor used by IMA. This is the rationale behind its degraded performance. Nevertheless, DAISY descriptor is much better in matching accuracy and that is the reason it is used in the IMA algorithm proposed in this paper. The least execution time recorded is 5.49 seconds for subject 4 of SURF algorithm. The highest execution time observed is 143.87 seconds taken by SIFT algorithm with subject 3. The execution time performance comparison is visualized in Figure 7.

There are different trends observed in the results of execution time for the five subjects and the average of them for all algorithms. The first observation is that execution time differed for each subject and each algorithm used in the experiments. It is because of the images captured with different lighting conditions, facial expressions, and timings as mentioned earlier in this paper. The second trend is that SURF showed superior

performance consistently for all subjects. In the same fashion, SIFT showed deteriorated performance for all subjects when compared with the other two algorithms. IMA showed consistently better performance over SIFT for all subjects but less than that of SURF. It is clearly reflected in the average of all subjects. The time taken for matching exhibited by IMA is 11.768 seconds which is much lesser than that of SIFT which took 81.616 seconds. The best performance is exhibited by SURF with 8.686 seconds execution time.

Table 3: Confusion matrix used for evaluation

	Ground Truth (matching)	Ground Truth (not matching)
Algorithm (matching)	True Positive (TP)	False Positive (FP)
Algorithm (not matching)	False Negative (FN)	True Negative (TN)

EVALUATION OF PROPOSED ALGORITHMS

The performance of the proposed methodology for detecting authorized RFID tag carrier in terms of tag and face image of the person who carried the tag is evaluated. Human experts are involved in the evaluation. Human experts observed the visitors to the smart building and compared with the registered RFID and face images manually. This has resulted in the ground truth. The ground truth values for all experiments are recorded. Then the same visitors have subjected to RFID based authentication which is an automated process. The results of the proposed algorithms TIA and IMA are compared against ground truth. Then the performance of IMA with respect to matching is compared with SIFT and SURF algorithms. Table 3 shows confusion matrix which is the basis for evaluation. Precision and recall are the measures used to evaluate performance of algorithms. They are computed as in Eq. 6 and Eq. 7.

$$\text{Precision} = (TP/(TP+FP)*100 \quad (6)$$

$$\text{Recall} = (TP/(TP+FP))*100 \quad (7)$$

Precision reflects the ratio of a number of correct matches to the total number of incorrect and correct matches. In the same fashion, recall is the ratio of a number of correct matches to the total number of correct matches present in the database. Both measures are inversely proportional. If precision increases, recall decreases and vice versa. Figure 8 shows the results of precision and recall measures for the smart building case study when RFID and face image are authenticated using TIA and IMA algorithms respectively.

The highest precision is exhibited by the proposed methodology containing IMA and TIA algorithms proposed in this paper. TIA with SURF and SIFT algorithms are compared with TIA with IMA. The least precision is exhibited by SURF algorithm. In a similar way, highest precision is shown by proposed approach. With respect to recall, least recall % is shown by SIFT and highest recall is shown by SURF algorithms.

Threats to Validity

The focus of this paper is to propose a methodology RFID based biometric access control for smart buildings. It is accomplished by defining two algorithms TIA and IMA that work together for authenticating RFID tag carrier. A model was built in Python for demonstrating proof of the concept. AT&T face image datasets are used for biometric authentication with image matching besides tag identification. The real life scenario is considered and laboratory experiments are made. Human experts are involved to prepare ground truth for experiments prior to testing the proposed methodology programmatically. The results are compared with existing algorithms and the efficiency of the proposed methodology is evaluated. A validity concern here is the ground truth provided by human experts. The quality of ground truth is influenced by the expertise of humans. There might be error rate that is not considered. There might be the problem with biased ground truth values as far as evaluation is concerned. Another important concern is that AT&T standard face image dataset is used for experiments. Though it contains 10 different variants of a face image, it may not reflect all kinds of facial expressions with different conditions in the real world. Therefore the ground truth derivation and dataset limitations are important threats to validity.

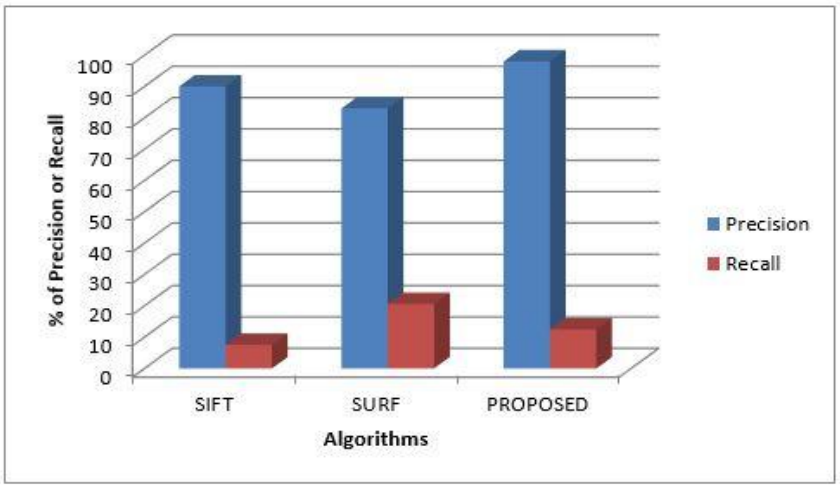

Figure 8: Precision and recall measures

CONCLUSIONS AND RECOMMENDATIONS

In this paper, we studied RFID based security to a smart building. RFID became a reliable for automatically identifying and tracking tags associated with objects in the real world. It can be used to have integration of physical and digital worlds. In the smart building case study, human beings (physical things) carry RFID tags that help them to participate in computations. The RFID tag carried by the human is subjected to verification up on receiving the tag information through tag reader. The two-fold authentication process is proposed as part of the methodology proposed in this paper. The methodology is meant for protecting the smart building from unauthorized access using RFID based mechanisms. We proposed two algorithms for this purpose. The first algorithm ACTIA makes verification of collision free RFID tag information while the second algorithm IMA uses the biometric measure known as face image matching. If authentication fails at ACTIA, there is no need for image matching as it can be concluded that unauthorized person is attempting to break security. In IMA algorithm DAISY descriptor is used which more accurate when is compared with SIFT and SURF. The performance of the three algorithms is evaluated in terms of average accuracy, average execution time, precision and recall. AT& T standard face image dataset is used for experiments. The results revealed the proposed methodology is effective with RFID based biometric authentication for protecting the smart building with secure access control. In future, we continue this research to have fully automated trust management in critical RFID applications.

REFERENCES

[1] Alqahtani S, Wamba SF, editors. Determinants of RFID technology adoption intention in the Saudi retail industry: an empirical study. System Science (HICSS), 2012 45th Hawaii International Conference on; 2012: IEEE.

[2] Wamba SF, Anand A, Carter L. A literature review of RFID-enabled healthcare applications and issues. International Journal of Information Management. 2013;33(5):875-91.

[3] Shaikh A, Al-Maymouni RK, Al-Hamed LH, Dardas A. The role of RFID in supply chain management macro processes. International Journal of Innovation, Management and Technology. 2014;5(5):388.

[4] Samad A, Murdeshwar P, Hameed Z. High-credibility RFID-based animal data recording system suitable for small-holding rural dairy farmers. Computers and electronics in agriculture. 2010;73(2):213-8.

[5] Brintrup A, Ranasinghe D, McFarlane D. RFID opportunity analysis for leaner manufacturing. International Journal of Production Research. 2010;48(9):2745-64.

[6] Marquardt N, Taylor AS, Villar N, Greenberg S, editors. Rethinking RFID: awareness and control for interaction with RFID systems. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems; 2010: ACM.

[7] Mokhsin M, Hamidi SR, Shaffiei ZA, Yaakop S. The Inventory Management System using RFID: Requirements Management. International Journal of Advanced Research in Computer Science. 2010;1(2).

[8] Ruiz-Garcia L, Lunadei L. The role of RFID in agriculture: Applications, limitations and challenges. Computers and Electronics in Agriculture. 2011;79(1):42-50.

[9] Baldini G, Oliveri F, Braun M, Seuschek H, Hess E. Securing disaster supply chains with cryptography enhanced RFID. Disaster Prevention and Management: An International Journal. 2012;21(1):51-70.

[10] Feldhofer M, Aigner M, Baier T, Hutter M, Plos T, Wenger E, editors. Semi-passive RFID development platform for implementing and attacking security tags. Internet Technology and Secured Transactions (ICITST), 2010 International Conference for; 2010: IEEE.

[11] Huang D, Zhang X, Kang M, Luo J, editors. MobiCloud: building secure cloud framework for mobile computing and communication. Service Oriented System Engineering (SOSE), 2010 Fifth IEEE International Symposium on; 2010: Ieee.

[12] Kim JT. Authentication Process between RFID tag and Mobile Agent Under U-healthcare System. Int J Bio-Sci Bio-Technol. 2014;6:109-16.

[13] Kurkovsky S, Syta E, Casano B, editors. Continuous RFID-enabled authentication and its privacy implications. Technology and Society (ISTAS), 2010 IEEE International Symposium on; 2010: IEEE.

[14] Zailani S, Iranmanesh M, Nikbin D, Beng JKC. Determinants of RFID adoption in Malaysia's healthcare industry: occupational level as a moderator. Journal of medical systems. 2015;39(1):172.

[15] Adhiarna N, Hwang YM, Park MJ, Rho JJ. An integrated framework for RFID adoption and diffusion with a stage-scale-scope cubicle model: A case of Indonesia. International Journal of Information Management. 2013;33(2):378-89.

[16] Vlachos IP. A hierarchical model of the impact of RFID practices on retail supply chain performance. Expert Systems with Applications. 2014;41(1):5-15.

[17] Smith AD. Case studies of RFID practices for competitive inventory management systems. Management Science, Logistics, and Operations Research: IGI Global; 2014. p. 1-25.

[18] Alfaro JA, Rábade LA, Rodríguez V. RFID technology as a strategic tool to improve inventory management: a case study. School of Economics and Business Administration, University of Navarra, 2010.

[19] Wright D. RFID and Wireless Personal Area Networks for Supply Chain Management. Encyclopedia of Mobile Computing and Commerce: IGI Global; 2007. p. 816-9.

[20] Lotfy MA. THE ROLE OF RFID IN THE SUPPLY-CHAIN: AN EDUCATIONAL CASE STUDY. Issues in Information Systems. 2014;15(2).

[21] Shin T-H, Chin S, Yoon S-W, Kwon S-W. A service-oriented integrated information framework for RFID/WSN-based intelligent construction supply chain management. Automation in Construction. 2011;20(6):706-15.

[22] Reyes PM, Worthington WJ, Collins JD. Knowledge management enterprise and RFID systems: Adoption to supply chain performance. Management Research Review. 2015;38(1):44-66.

[23] Bembenek B. RFID within High-Tech Clusters–Towards a Knowledge-Based Economy. Economics and Business. 2016;28(1):52-60.

[24] Srivastava B. Critical management issues for implementing RFID in supply chain management. International Journal of Manufacturing Technology and Management. 2010;21(3-4):289-307.

[25] Zuo Y, Pimple M, Lande S. A Framework for RFID Survivability Requirement Analysis and Specification. Innovations in Computing Sciences and Software Engineering. 2010:153-9.

[26] Bendavid Y, Bourgault M. A living laboratory for managing the front-end phase of innovation adoption: the case of RFID implementation. International Journal of Project Organisation and Management. 2010;2(1):84-108.

[27] Ferrer G, Dew N, Apte U. When is RFID right for your service? International Journal of Production Economics. 2010;124(2):414-25.

[28] Lollar JG, Beheshti HM, Whitlow BJ. The role of integrative technology in competitiveness. Competitiveness Review: An International Business Journal. 2010;20(5):423-33.

[29] Quetti C, Pigni F, Clerici A. Factors affecting RFId adoption in a vertical supply chain: the case of the silk industry in Italy. Production Planning & Control. 2012;23(4):315-31.

[30] Garrido Azevedo S, Carvalho H. Contribution of RFID technology to better management of fashion supply chains. International Journal of Retail & Distribution Management. 2012;40(2):128-56.

[31] Chan FT, Chong AY-L. Determinants of mobile supply chain management system diffusion: a structural equation analysis of manufacturing firms. International Journal of Production Research. 2013;51(4):1196-213.

[32] Fawcett SE, Jones SL, Fawcett AM. Supply chain trust: The catalyst for collaborative innovation. Business Horizons. 2012;55(2):163-78.

[33] M. Beheshti H, K. Blaylock B, A. Henderson D, G. Lollar J. Selection and critical success factors in successful ERP implementation. Competitiveness Review. 2014;24(4):357-75.

[34] Ahmadi H, Nilashi M, Ibrahim O. Prioritizing critical factors to successful adoption of total hospital information system. Journal of Soft Computing and Decision Support Systems. 2015;2(4):6-16.

[35] Yao W, Chu C-H, Li Z, editors. The use of RFID in healthcare: Benefits and barriers. RFID-Technology and Applications (RFID-TA), 2010 IEEE International Conference on; 2010: IEEE.

[36] Lewis MO, Balaji S, Rai A, editors. Rfid-Enabled Capabilities and their Impact on Healthcare Process Performance. ICIS; 2010.

[37] Terziyan V, Kaykova O, Zhovtobryukh D, editors. Ubiroad: Semantic middleware for context-aware smart road environments. Internet and web applications and services (iciw), 2010 fifth international conference on; 2010: IEEE.

[38] Cusack B, Ayaw AK. Evidential Recovery in a RFID Business System. 2010.

[39] Prasad N, Rajesh A. RFID-Based hospital real time patient management system. International Journal of Computer Trends and Technology. 2012;3(3):1011-6.

[40] Mubarak MF, Yahya S, editors. Mutual attestation using TPM for trusted RFID protocol. Network Applications Protocols and Services (NETAPPS), 2010 Second International Conference on; 2010: IEEE.

[41] Monahan T, Fisher JA. Implanting inequality: Empirical evidence of social and ethical risks of implantable radio-frequency identification (RFID) devices. International journal of technology assessment in health care. 2010;26(4):370-6.

[42] Peng K, Bao F. A secure RFID ticket system for public transport. Data and Applications Security and Privacy XXIV. 2010:350-7.

[43] Li M, Huang M-Y. Trust Management Framework for Ubiquitous Computing Applications. AIAA Infotech@ Aerospace 20102010. p. 3314.

[44] Liu H, Ning H. Zero-knowledge authentication protocol based on alternative mode in RFID systems. IEEE Sensors Journal. 2011;11(12):3235-45.

[45] Yang J, Wang Y, Cai Q, Zhan Y. A novel hybrid anticollision algorithm for RFID system based on grouped dynamic framed recognition and binary tree recursive process. International Journal of Distributed Sensor Networks. 2015;11(8):641327.

[46] Bunduchi R, Weisshaar C, Smart AU. Mapping the benefits and costs associated with process innovation: The case of RFID adoption. Technovation. 2011;31(9):505-21.

[47] Abowd G, Dey A, Brown P, Davies N, Smith M, Steggles P, editors. Towards a better understanding of context and context-awareness. Handheld and ubiquitous computing; 1999: Springer.

[48] Bringer J, Chabanne H, Icart T, editors. Cryptanalysis of EC-RAC, a RFID Identification Protocol. CANS; 2008:

Springer.

[49] Good T, Benaissa M. A holistic approach examining RFID design for security and privacy. The Journal of Supercomputing. 2013;64(3):664-84.

[50] Molnar D, Soppera A, Wagner D, editors. Privacy for RFID through trusted computing. Proceedings of the 2005 ACM workshop on Privacy in the electronic society; 2005: ACM.