Proc. of The Seventh International Conference on Advances in Computing, Electronics and Communication - ACEC 2018

ISBN: 978-1-63248-157-3 doi: 10.15224/978-1-63248-157-3-07

An Integrated System for the Issuance of e-Passports

Husna Gul A.Wahab[1], Muhammad Taha Jilani[2], Muhammad Khalid Khan[3], Mohammad Fadzil Hassan[4]
[1,2,3]Graduate School of Science and Engineering,
Pakistan Air Force Karachi Institute of Ecnomics and Technology, Karachi, Pakistan
[4]Department of Computer and Information Sciences, Universiti Teknologi PETRONAS, Malaysia

***Abstract*— Recent developments in information and communication technologies (ICT) have more impact on humans lifestyle and society, than ever before. However, in the most of the developing countries, still the potential of ICT has not been fully utilized, due to lack of infrastructure, limited resources and the higher cost. This ultimately possesses a burden on governments and regulating agencies to perform citizen's related matters inefficiently. This paper presents a simple and low cost but yet effective, IoT based system for the issuance of e-passports to the citizens. The proposed system mitigates the time consuming traditional practices and the unnecessary involvement of human resources, thus it provides a fast, simple and low cost solution to the regulating authorities. The whole process from applying for passport to verification of credentials and issuance of passport can be done with the kiosk installed across the metropolitans and remote areas. The system is integrated with sensors and the customized application provides a user friendly interface to the applicants. It is equipped with secure transmission of data while security mechanism is also incorporated within the system.**

Keywords*— *Internet-of-things, Service-Oriented Architecture, e-Passports, COAP.

I. Introduction

In the last few years, the progressive developments in information and communication technologies (ICT) have more impact on human's lifestyle and the society than ever before. This has been realized with a cognitive environment especially formed for computation by a collection of several interconnected sensors or devices [1]. These devices or sensors can communicate with each another through network or internet to exchange data, hence, it becomes easy to manage and control services within the distributed environment, which is now known as Internet-of-Things. With IoT, the growing inter connectivity of devices has made possible to realize the real-time services on everywhere and anytime basis, and these services are not only use for machines but among humans too[2]. According to the Cisco Internet Business Solutions Group (IBSG), the IoT was introduced between 2008 and 2009, and as predicted by 2020 there will be approximately fifty billion devices which will have Internet connectivity [3].

Elements of Internet of things defined in [4] are things, gateway, cloud and enterprise. As IoT is being used in enterprises, it is now transforming the traditional system into smart systems and it geared to achieve computation and communication in anything, anywhere and anytime [5].

In developing nations, such as Pakistan, with the population of about 207.74 million the issuance of passport is really a complex task for the citizens. The system is being monitor and control by the Immigration & Passports department, under the ministry of interior, government of Pakistan. Since, the whole system is based on manual data entry and verification procedures by the staff and the limited number of offices across the country, it becomes a cumbersome to both citizens and the government to manage and control it efficiently. Even, the residents of remote areas and villages are needs to travel the metropolitans to just obtain their passports. The current system takes more time to apply for passport, since all the things from time reservation to document submission are being manually handled, users have to go through the process by visiting many people who are serving the applicants by taking their biometric, personal data or photographs etc. The manual passport makes the whole process very slow, that can even take days because mostly it cannot be done in a single visit. So there should be a smart passport issuance system which will provide services in less time but more efficiently and the system must be easily understandable for applicant.

II. Literature Review

For the development of large national identification system (or any similar system) there are multiple methods have been proposed before for range of applications. In the most of these systems the users authentication and registration is based on biometric verification. In such systems the identity or the uniqueness of a person on the basis of one's biometric parameters such as, fingerprints, face recognition, retinal and iris scanning, can be used for verification purposes since they differs person to person [6]. The operation of such systems usually follows the standard sequence [7]:

- First of all it will capture the data from biometric sensor.
- After capturing sensor's data, it is converted into intermediate form by extracting features from raw sensor's data.
- Then the template is created from extracted data for the purpose of storage.
- For verification purpose, stored template can be compare with the input data.
- In [8] e-passport's structure includes two things
- Traditional Text Information (It includes ID of passport holder, Name of passport holder, country place of birth etc.)

- Personal Bio-information(It includes sample of DNA of passport holder, Iris pattern, fingerprint of passport holder).

A framework of internet voting were presented in 2005 in Estonia [9], which was consisted of Client side and Server side. The election commission also provided an application for voter, so that a voter confirms his or her vote. First of all voter can cast the vote through web after casting the vote QR code is shown at the screen, voter can scan this code by the QR reader which is available in the application provided by election commission. Once user confirms it, then it will be stored in database which is in server side.

Another electronic voting system's framework proposed in [10], applicant can cast his or her vote by laptop, smart phone, or any other smart device. Internet is the essential need of this framework through internet the casted votes are stored in database.

In both cases Instead of using manual voting system a smart voting system was introduced. Which saves the time of voter as well as the voter must not have to stand in queue for a long time so human effort is also saved by this smart system. But there are some limitations which are also available in both system like security threat. Vote of the voter is discarded by an attacker or an attacker can caste a false vote etc.

III. Methodology

The proposed IoT based integrated system for the issuance of e-passport will be developed with a kiosk, equipped with NFC reader, camera, microphone, keypad and the touch interface. The whole process of e-passport issuance in this is divided into couple of steps:

A. *First Step*

Applicant has two options renew the passport or apply for the passport for first time, for both process, application reservation of token is required. For Token reservation an account is needed as shown in Figure 1, which can be created with the national identification card (NIC) and email. NIC must be taken as the user name so that one NIC can create only one ID. Once applicant creates an account and apply for token it will provide two things to applicant, (i) Token which is generated automatically by system which will be used for verification at the time of applying for passport (ii) Time slot for applying or availing the service.

B. *Second Step*

After reserving the token, the applicant can use service at that time which the reservation system provided to that applicant. Applicant can enter Token, smart machine will verify the token first by checking/verifying the token which is entered by user is valid and secondly it will check the time if the provided time matches with current time then service will be provided otherwise not. If token is verified, two options will be showed to applicant (a) First time (b) Renew. However, in the case of passport renew one of these two condition must be true: (a) passport is going to be expired in next seven month, or (b) expired passport.

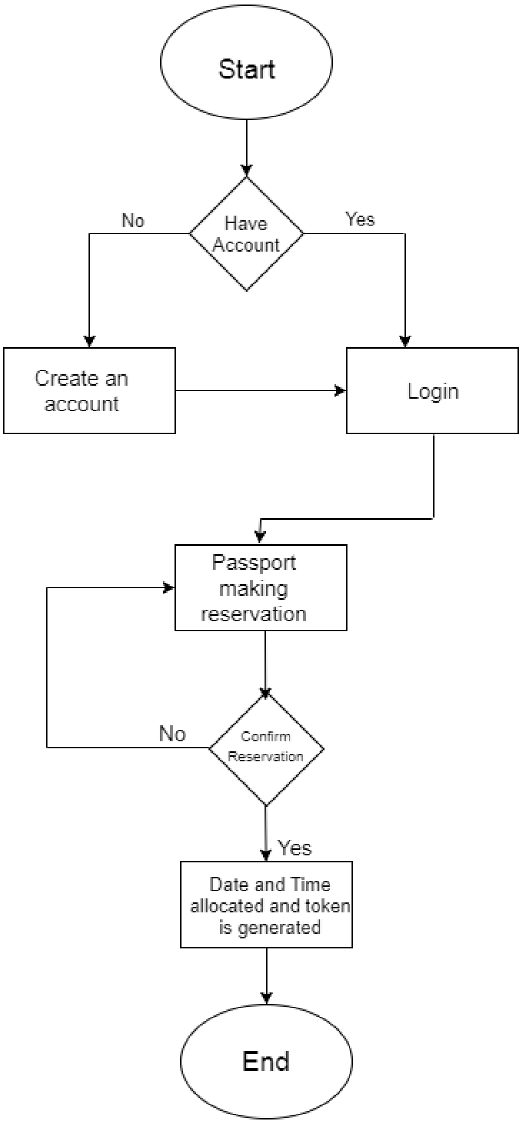
Start
Have Account
No
Yes
Create an account
Login
Passport making reservation
Confirm Reservation
No
Yes
Date and Time allocated and token is generated
End

Fig. 1. Steps for a slot reservation

C. *Third Step*

Applicant can pay the fee or charges of making passport online by providing the debit/credit card no. or applicant can pay the charges through NFC based mobile payment. In our smart system there are NFC reader. Two devices containing NFC chips can communicate and exchange data within few centimeter. In our smart system it is one way communication which is just reading NFC data as it is defined here.

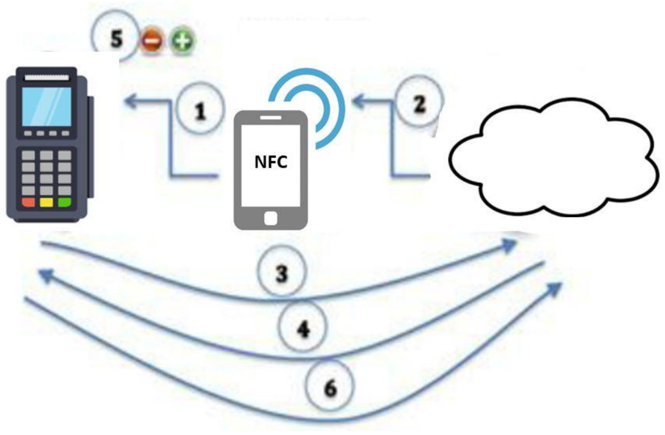

Fig. 2. Mobile payment through NFC in six steps

As shown in Figure 2, model of NFC wallet along with cloud follow these steps [11]:

1) NFC based mobile is waved at the NFC reader by applicant for the purpose of payment.

2) Application which is for payment is downloaded in applicant's mobile SE.

3) NFC reader checks that applicant's account contains the required amount or not by communicating with cloud partner.

4) Required data is transferred to the NFC Reader.

5) At this point NFC reader can either reject or accept the transaction on the basis of provided data by cloud partner.

6) Amount will be deducted after confirmation that the transaction is authenticated, authentication is done by RFC reader communication with cloud partner.

D. *Fourth Step*

For document submission, scanner scans the documents which are required for applying for passport. Applicant can be an employee of government or normal civil citizen. Civil citizen is further divided by age below eighteen and above eighteen. Documents for each type of user are shown in Figure 3-5.

E. *Fifth Step*

Camera is embedded in system which is placed above the screen of smart system, which clicks the photo of applicant. Demonstration through multimedia or voice of picture clicking is showed to applicant to fulfill the requirements.

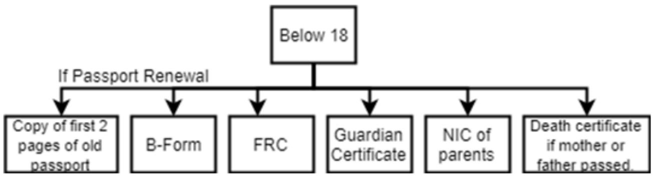
Below 18
If Passport Renewal
Copy of first 2 pages of old passport
B-Form
FRC
Guardian Certificate
NIC of parents
Death certificate if mother or father passed

Fig. 3. Documents required for below 18 (civil citizen).

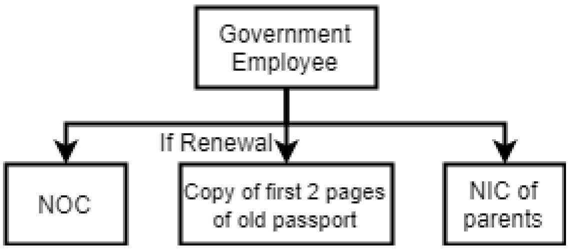

Fig. 4. Document required for Government officer

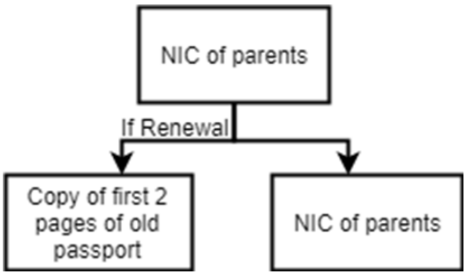

Fig. 5. Documents required for above 18(civil citizen)

F. *Sixth Step*

Below the screen there is another sensor of biometric which is used for capturing fingerprints of applicant. Demonstration through multimedia or voice of using fingerprint sensor is showed to applicant to fulfill the requirements.

Working of a biometric system along with verification from NADRA database is shown in Figure 6 [12]. Further, the feature extraction of a biometric data [13], is also presented in in Figure 7. The whole process follows

- First of all user put the finger on the sensor.
- Optical scanner is used to scan the finger print and Sensor will extract the features of finger prints.
- Extracted feature is then compared with the saved template which is in the database of National Database & Registration Authority (NADRA), if it matched then the user is authenticated otherwise process will be discarded.

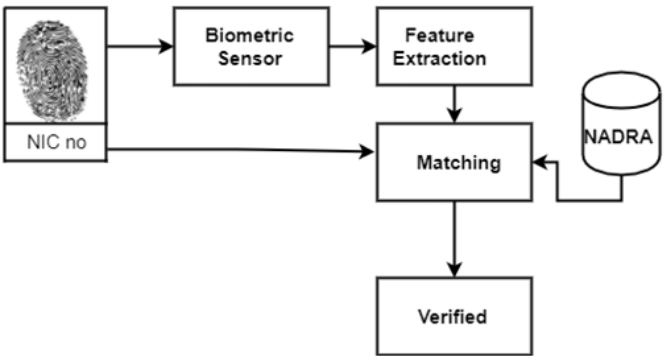

Fig. 6. Biometric verification system

G. Seventh Step

Applicant verification is being done as this stage while the other data like finger prints are also verified at this stage by National Database and Registration Authority (NADRA).

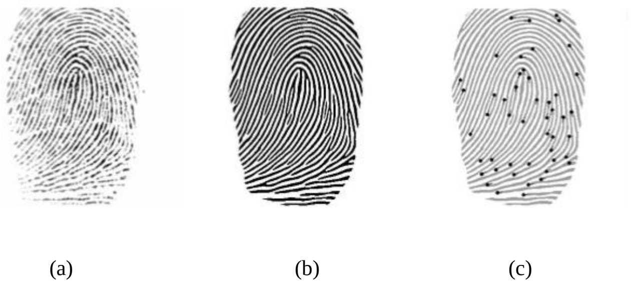

Fig. 7. Feature Extraction Process (a) original (b) after process (c) alongwith feature points

H. Eighth Step

If applicant's record is cleared and verified by each and every department as discussed above then application can be submitted otherwise applicant must have to fulfill the requirement to process further. Finally, once the process is completed, the prepared e-passport will be delivered to the person's home.

IV. Proposed Architecture

In literature there are multiple types of architecture has been discussed for an Internet-of-Things based network. The most of the popular architecture are describe below:

A. Three layered Architecture

In [14-16] the simplest model of internet of things contains these layers which are:

- Application Layer: Interface for user is provided.
- Network Layer: Transmits the data which is collected by sensors through a medium like 4G etc.
- Perception Layer: Sensors etc.

B. Five Layered Architeture

More than 3 layer architecture of internet of things discussed in [14-16] are

- Business: Charts related to service of internet of things i.e. application flow etc.
- Application: Provide requested services for user.
- Service Management: Coder is allowed to program with the objects which are heterogeneous without bounding to a single platform.
- Object Abstraction: Data collected by sensors is transferred to its upper layer through GSM, WLAN etc.
- Object: Sensors, Actuators, etc.

C. Service Oriented Architecture

In [17] SOA architecture is designed which is consist of following layers

- Interface Layer: User Interface
- Service Layer: Service Division, Service Integration, Service Composition.
- Network layer: Social Network, Mobile Network etc.
- Sensing Layer: Sensors.

In [18] a SOA based middleware architecture has been discussed, layers of this middleware are shown in Figure 8.

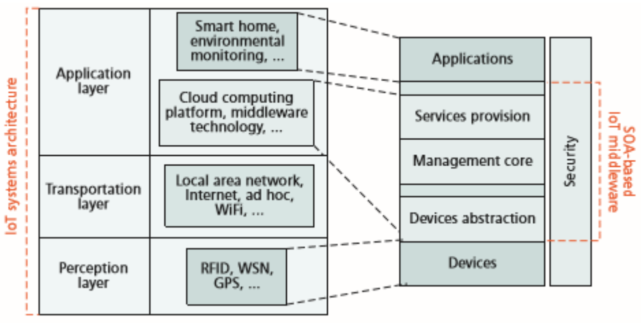

Fig. 8. SOA-middleware architecture[5]

D. Proposed System Architecture:

SOA Based IoT middleware is the most suitable choice of architecture for smart passport issuance system. Reason of choosing middleware is as smart system is inter linked with National Database and Registration Authority and Federal Board of Revenue for the purpose of verification to avail the services. So middleware allow us to interconnect with other smart systems too which is the need of our architecture. Resources are shared among systems through middleware. Purpose of choosing the Service Oriented Architecture is it divides the complex system into sub system which can be reused and also these sub system can be upgraded efficiently.

TABLE I. IoT Stacked Layers Responsibilieties

Layer	**Responsibilities**
Application	Services are provided to applicant i.e. an applicant wants to make a new passport so smart system shows the complete procedure.
Service	Two sub layers can be found in this layer • Service Management: Maintenance of every sensor's data is taking place in this sub layer for example few sensors which are embedded in smart system are RFID reader, fingerprints

Copyright © Institute of Research Engineers and Doctors, USA. All rights reserved.
ISBN: 978-1-63248-157-3 doi: 10.15224/978-1-63248-157-3-07

	etc., the data of these sensors are managed here. In addition the data of these sensor are further processed to make decisions. •Service Composition: As the name of this sub layer, there is composition of particular sensor like data of biometric sensor is used for verification of individual.
Data Abstraction	Interface is provided for the management of all incoming and outgoing communication through internet. For example our smart system send request to NADRA of FBR DB all the communication is being monitored and managed by the interface.
Sensing	All the sensors providing services in whole smart systems are included in this layer for example RFID reader, finger print sensor, camera etc.

E. Application Level Protocol:

For Smart Passport System CoAP [19], which stands for Constrained Application Protocol is the best application level protocol. In this protocol there is Request and Response mechanism and also a lightweight protocol with low overhead than other protocols which is the need of proposed smart system. Request in proposed system i.e. biometric sensor data for verification, NFC mobile payment request must be Confirmable and in the result response must be synchronized.

V. Security

Technologies which are used in this smart system are biometrics, which are vulnerable in few aspects. Biometrics vulnerability [20], can be classified into two categories.

- Intrinsic Failure: Reason of this failure is improper decision which is taken by system.
- Biometric failure: This failure is due to the attacks which are launched by an opponent.

The most important thing to protect in biometric system are templates of biometric. How to save these templates in database so that no opponent can access it and misuse it for this purpose some techniques are available like salting, hashing etc.

A. Data privacy

Data privacy of applicant is an essential part of smart system because of the privacy issue many user don't accept the smart systems. In smart passport issuance system there are critical data related to applicant which are fingerprints, NIC number, Credit card number and other data. So privacy of user data is mandatory because if this data is compromised then there will be lots of losses. Because all the data are taken online, encryption of data and template of biometric is necessary and hashing is the best choice for it. DOB and NIC number (it is unique) will be used as the key for hashing, hashing technique is chosen for encryption because of its noninvertible feature. In case an opponent gets the key still cannot decrypt the data.

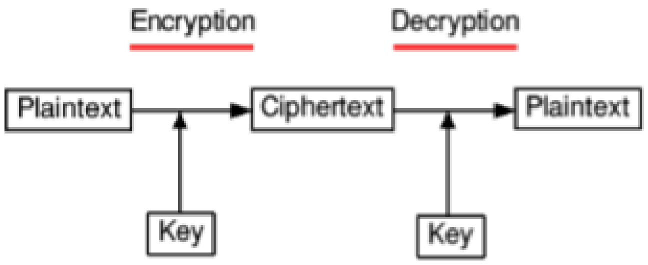

Fig. 9. Data Security to retain user confidentiality and privacy

B. Securley access of national databases

In smart system data exchange with national databases, such as NADRA and FBR, will take place. The transmission between smart system and these databases must be secured to prevent attacks by unauthorized person. As reported in [21], this data must be encrypted and in the case of attack, the confidentiality of data must be retained (Figure 8).

In this proposed smart system, AES-256 seems to be the best choice. It is a symmetric Cipher which uses the same key for encryption and decryption. Key is 256 bit long, it contains 14 repetition cycle, and each cycle contain several steps of processing. More rounds there will be in an algorithm so more data will be secure. Key is known by sender and receiver end. NIC plus DOB of applicant number is used as unique key for every individual citizen.

When smart system send request to NADRA or FBR, the data which is used to make a request is encrypted by AES-256. At the second end NADRA or FBR decrypt the data with the shared key and reply the request. Data which is retrieved in the result of request is encrypted and transfer to smart system, finally the smart system decrypt the data.

VI. Comparative Analysis

This section presents the comparison of the proposed system with the traditional system. The comparison is based on three main parameters, namely cost, time and human involvement.

A. Cost

If the proposed system is compared with the traditional system, it costs more than smart system. One of the important aspect is the group of staff and related officers that are serving applicants. The expenditures for that group (ranging from 25 to 30 persons) will be much higher than operational and maintenance cost of the proposed system.

As it is known that sensors required for the process of making passport are available even in normal system, all these sensors are being used but along with the interference of humans. What if we integrate these sensors, in the result we have a smart machine which work more efficiently with less cost. Similar approach has been used somewhere, but in different context [22].

Proc. of The Seventh International Conference on Advances in Computing, Electronics and Communication - ACEC 2018
Copyright © Institute of Research Engineers and Doctors, USA. All rights reserved.
ISBN: 978-1-63248-157-3 doi: 10.15224/978-1-63248-157-3-07

B. *Processing Time*

In normal passport system the making of passport is really a tough job which consume a lot of time as there are 6 corners where an applicant must have to go and provide information or perform the intended task. Sometime this process becomes too long that it can be complete into one to three visits.

The most time consuming part of the whole procedure is reservation of token because of manual system there are queue of people which are too long. But in smart system every step is taking less time than the normal passport system as it is shown into Table 2.

C. *Human Involvement*

Smart system works faster because of no human involvement. Sometime human involving creates trouble as it is known that there is limit of human work or energy so because of it human can't handle many people at same time, in the result more time is required to process the whole procedure. Applicant can faces delay in the process. Due to human involvement the cost and time increase.

TABLE II. PERFORMANCE COMPARISON WITH TRADITIOANL SYSTEM

No	**Processing Time**		
	Activity	***Traditional System (mins)***	***Smart System (mins)***
1	Reservation of token	60	2
2	Submission of documents	30	5
3	Fingerprints capturing(biometrics)	15	3
4	Picture clicking	15	2
5	Verification(NADRA etc.)	15	3
6	Application submission	15	2
	Total	150 mins	17 mins

VII. CONCLUSION

In this paper a smart system for the issuance of e-passport is proposed which can outperforms the traditional system. Based on IoT, it will provide a more comprehensive solution to the governments and the authorities. By adopting a smart e-passport system, authorities can manage this time and resource consuming procedure in a simple, low cost, hassle-free but yet effective manner. Similarly, for the citizens it will give them opportunity to obtain their passports in a more flexible way. It mitigates the time consuming traditional practices and the unnecessary involvement of human resources, thus provides a fast, simple and low cost solution. A SOA-based middleware approach has been adopted while an integrated system is proposed that can even work in a distributed environment. The whole process from applying for passport to verification of credentials and issuance of passport can be done with the kiosk installed across the metropolitans and remote areas. By comparing with traditional method it is found that the proposed system reduces the processing time of an each user significantly.

REFERENCES

[1] A. Ukil, J. Sen, and S. Koilakonda, "Embedded security for Internet of Things," in *Emerging Trends and Applications in Computer Science (NCETACS), 2011 2nd National Conference on*, 2011, pp. 1-6.

[2] F. Xia, L. T. Yang, L. Wang, and A. Vinel, "Internet of things," *International Journal of Communication Systems*, vol. 25, p. 1101, 2012.

[3] D. Egan, "The emergence of ZigBee in building automation and industrial control," *Computing & Control Engineering Journal*, vol. 16, pp. 14-19, 2005.

[4] K. S. Munasinghe and A. Jamalipour, "Interworked WiMAX-3G cellular data networks: an architecture for mobility management and performance evaluation," *IEEE Transactions on Wireless Communications*, vol. 8, pp. 1847-1853, 2009.

[5] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, pp. 2787-2805, 2010.

[6] B. Schouten and B. Jacobs, "Biometrics and their use in e-passports," *Image and Vision Computing*, vol. 27, pp. 305-312, 2009.

[7] S. Kundra, A. Dureja, and R. Bhatnagar, "The study of recent technologies used in E-passport system," in *Global Humanitarian Technology Conference-South Asia Satellite (GHTC-SAS), 2014 IEEE*, 2014, pp. 141-146.

[8] J. Yong and E. Bertino, "Replacing lost or stolen E-passports," *Computer*, vol. 40, 2007.

[9] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, *et al.*, "Security analysis of the Estonian internet voting system," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014, pp. 703-715.

[10] E. Aljarrah, H. Elrehail, and B. Aababneh, "E-voting in Jordan: Assessing readiness and developing a system," *Computers in Human Behavior*, vol. 63, pp. 860-867, 2016.

[11] P. Pourghomi and G. Ghinea, "A proposed NFC payment application," *arXiv preprint arXiv:1312.2828*, 2013.

[12] O. Akinola, A. Abayomi-Alli, and R. Adeniyi, "Development of a Microcontroller Based Fingerprint Examination Access Control System," 2015.

[13] T. C. Clancy, N. Kiyavash, and D. J. Lin, "Secure smartcardbased fingerprint authentication," in *Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications*, 2003, pp. 45-52.

[14] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in *Frontiers of Information Technology (FIT), 2012 10th International Conference on*, 2012, pp. 257-260.

[15] Z. Yang, Y. Yue, Y. Yang, Y. Peng, X. Wang, and W. Liu, "Study and application on the architecture and key technologies for IOT," in *Multimedia Technology (ICMT), 2011 International Conference on*, 2011, pp. 747-751.

[16] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of Internet of things," in *Advanced*

ISBN: 978-1-63248-157-3 doi: 10.15224/978-1-63248-157-3-07

Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, 2010, pp. V5-484-V5-487.

[17] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," *Information Systems Frontiers*, vol. 17, pp. 243-259, 2015.

[18] R. T. Tiburski, L. A. Amaral, E. De Matos, and F. Hessel, "The importance of a standard securit y archit ecture for SOA-based iot middleware," *IEEE Communications Magazine,* vol. 53, pp. 20-26, 2015.

[19] C. Bormann, A. P. Castellani, and Z. Shelby, "Coap: An application protocol for billions of tiny internet nodes," *IEEE Internet Computing,* vol. 16, pp. 62-67, 2012.

[20] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on advances in signal processing,* vol. 2008, p. 113, 2008.

[21] P. K. Singh, P. Tripathi, R. Kumar, and D. Kumar, "Secure Data Transmission," *International Research Journal of Engineering and Technology,* vol. 4, pp. 217-222, 2017.

[22] M. M. B. Baig and M. T. Jilani, "An iBeacon based Real-time context-aware e-healthcare system." *IEEE First International Conference on Latest trends in Electrical Engineering and Computing Technologies (INTELLECT),* 2017.