A Vision Based Three-Layer Access Management System with IoT Integration

Nafize Ishtiaque Hossain
Department of Electrical and Electronic Engineering
Chittagong University of Engineering and Technology
Chittagong, Bangladesh
nafize.ishtiaque@gmail.com

Ali Reza Galib
Department of Electrical and Electronic Engineering
Chittagong University of Engineering and Technology
Chittagong Bangladesh
argalib.ac@gmail.com

Raihan Bin Mofidul
Department of Electrical and Electronic Engineering
Khulna University of Engineering and Technology
Khulna, Bangladesh
raihanbinmofidul@outlook.com

Dhiman Kumar Sarker
Department of Electrical and Electronic Engineering
Chittagong University of Engineering and Technology
Chittagong, Bangladesh
sagor.eee.cuet@outlook.com

***Abstract*— In developing countries, traditional access management systems ubiquitously use either keypad based password protection or radio frequency identification (RFID) card based protection. With the increased number of threats in recent years, these systems are becoming more vulnerable. If the password or the RFID card is somehow compromised, any unauthorized person can breach the system with ease. Considering and analyzing these issues, a cost-effective prototype of a vision based three-layer access management system with IoT connectivity was developed. In this paper, an access management system architecture is proposed based on the fusion of radio frequency identification, back propagation based face recognition and password protection. The system is also connected to a Node JS based web server. Whenever an access is granted or any unauthorized access is detected, an SMS and an email are sent to both the user and the system administrator. Data security is ensured by exploiting AES encryption on the system side and AES decryption on the server side. In case of face recognition, the access is granted if the achieved confidence level is over 80%.**

Keywords—AES encryption; back propagation; face recognition; Node JS; password; RFID;

I. INTRODUCTION

In today's world, significant priorities are being given to research and development of secure access management systems. As the level of security increases, the cost of systems increases accordingly. In developing countries like Bangladesh, it is quite overwhelming for small businesses and corporations to afford high-level and complex security systems. In most small businesses, access control systems are either based on password or radio frequency identification (RFID) cards or a combination of both. But it is seen that most of the time the access systems are quite vulnerable to potential threats. Unauthorized access is possible if the password or the RFID card or both are compromised somehow. To prevent such an inconvenience, a three-layer authentication based cost-efficient access control system integrating the internet of things (IoT) environment is developed. In section II literature review, section III system architecture, and section IV software architecture is described. Section V, VI and VII describe performance evaluation, comparative analysis and conclusion respectively.

II. LITERATURE REVIEW

Face recognition and gait analysis based identification system for access control is shown in [1]. From a video, at first human detection is done then after background subtraction and human silhouette, the silhouette is normalized to analyze a gait. Both frequency representation and binary representation is shown in [1]. Research in [2] shows face, fingerprint and palm vein based biometric security systems for the internet of medical things (IoMT) platform. A noninvasive and continuous biometric signal collection, as well as authentication from wearable medical device for access control, are shown in research [3]. Smart card based control system where all system data is protected by cryptography is proposed in a research [4]. A near field communication (NFC) and digital signature based access control system is in literature [5]. Here the access is granted after the validation of NFC and digital signature. Electromagnetic lock and modified RFID based system was also shown in some research [6] where electromagnetic lock is interconnected with a system which will grant access for some specific RFID tag. An artificial neural network (ANN) controlled face recognition based access control system has been developed recently [7]. Local binary pattern based face recognition for access control is developed in [9] were after conversion to binary image, analysis of the pattern of the binary image is done for face recognition. An FNN and RFID based access system for internal use is shown in research [8]. A stereo face recognition system is proposed previously by some researchers [10] which can be implemented only in low light indoor environment. Principle component analysis based face recognition is shown in some access systems [11] where the captured image can be seen from a web browser and at same time, a GSM modem sends this information to the user and the administrator. The incorporation of password, fingerprint and RFID card for several stage authentications is implemented in one of the recent researches [12]. PCA and back propagation based face recognition is shown in some

research [14] which can be very useful in future access control system. Again, logistic regression based face image recognition can be a potential resource to use in accesses control systems. In [15], a smart phone application based smart lock system is introduced.

III. System Architecture

The proposed system hardware includes a raspberry Pi 3, an RFID reader, a USB webcam, and a 4X4 keypad. The system block diagram is given in the following Fig. 1.

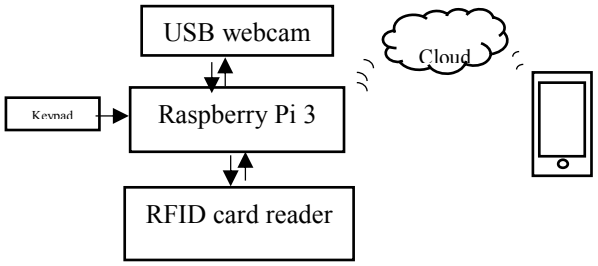
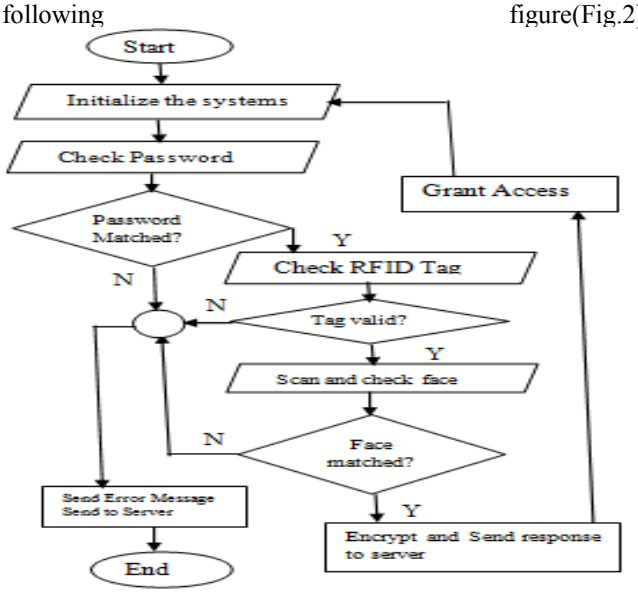


Fig. 1. System Architecture

The main processing part of authentication system is done in the Raspberry Pi 3, which is a single board computer with 1GB RAM, and the Linux operating system. To reduce power consumption, a 125kHz passive RFID tag is used and a low power RFID reader RDM600 [16] is connected with the Raspberry Pi 3 via serial communication, where the baud rate was 9600. The resolution of the USB web cam is 5M pixels, and the frame rate is 60fps. The focal length is manually adjustable from 3.5cm to 8cm. A lin-log CMOS image sensor is used in this camera.

If the user wants to access the facility, at first, the password has to be given via the keypad. After that, an RFID card has to be placed in front of the RFID reader. If the RFID card and the password are matched, then the face of the user will be scanned via the USB webcam. If all three of the systems are matched with the stored data, then the access is granted and an AES encrypted grant response is sent to the Node JS based cloud server. Upon receiving this message and decrypting it, the web server will send a verification SMS to the user and a notification SMS to the system administrator. The flow chart of the system is given in the following figure(Fig.2).



. Fig 2. Flow chart for access management

If any one of the step is mismatched, the system will send an error message to the web server which will be encrypted too. When the web server receives the error message, it will send an alert SMS to both the user and the administrator.

IV. Software Development

The software development can be divided into two main parts and they are system side software development and the server side software development. These two developments are described in the following two sub sections. The system side software was developed with python language and the server side software was developed in Node JS platform.

A. System Side Software Development

The main architecture of the software is based on the flow chart shown in the figure 2. The password verification, RFID match, and face recognition is employed via polling algorithm. The main section of the flow chart is the face recognition part. To recognize the face, back propagation based neural network is employed. At first, the image is captured and the face is detected. Then, the image is converted in to grayscale image. After that feed forward propagation is employed where each node of the network is characterized by sigmoid function denoted by,

$$g(x) = 1/(1+\exp(-z)) \quad (1)$$

Since sigmoid function is used, it has the probability to meet at the local minima so the modified cost function is defined as

$$J(\theta) = (1/m) * \{\Sigma\, y^{(i)} \log[g(x^{(i)})] + (1-y^{(i)}) \log[a-g(x^{(i)})]\} \quad (2)$$

The learning rate is chosen such that it is neither too small nor too large. If the learning rate is high, it has the risk to overshoot the minima. On the other hand, if the learning rate is too small then the it will cause prolonged convergence making the system impractical. To prevent oscillation, the momentum factor is chosen accordingly. The learning rate and momentum **f**actor took part in the modification of the weight.

The activation function of any layer is a_j^l and denoted by

$$a_j^{(l)} = g(\Theta^T.x) \quad (3)$$

Here Θ is the weight vector and Θ^T is the transpose of the weight vector.

If the error in jth node in layer l is denoted by

$$\delta_j^{(l)} = (\Theta^{l)\,T}\, \delta_j^{(l-1)}\ .\ *g^l(z^l) \quad (4)$$

Where $g^l(z^l) = a^{(l)}\ .*(1-a^{(l)})$.

After computing the error term, $\Delta_{i,j}^l$ will be modified as

$$\Delta_{i,j}^l := \Delta_{i,j}^l + a_j^{(l)}\, \delta(l\text{-}1) \quad (5)$$

Fig. 3.Face recognition dataset.

B. *Server Side Software Development*

The server side software development is more straight forward. In this development, a Node JS based IBM's server is used. In the subsequent two blocks after the decision taking block namely error response block in the flow chart in Fig. .4, Twilio's API is used for sending SMS to the user and the administrator. MongoDB API used for server side database development. It is realized by the following flow chart.

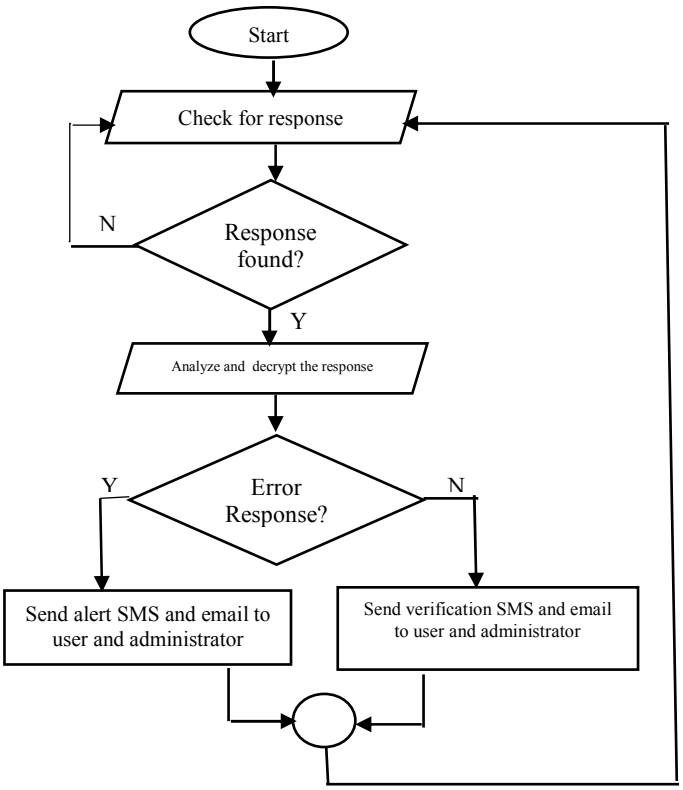


Fig. 4. Flow chart for web server side development

The practical implementation of the automated SMS and email in response to the defined situation is shown in the Fig. 5. The first two sub figures are email responses from the web server to the user about access notification and alert notification (Fig 5(a) and Fig 5(b)). The third sub figure is the SMS response to the user which notifies them about suspicious activity in their residence. (Fig 5c). Authorized face recognition and access management system hardware setup is shown in Fig. 6 and Fig. 7 respectively.

V. PERFORMANCE ANALYSIS

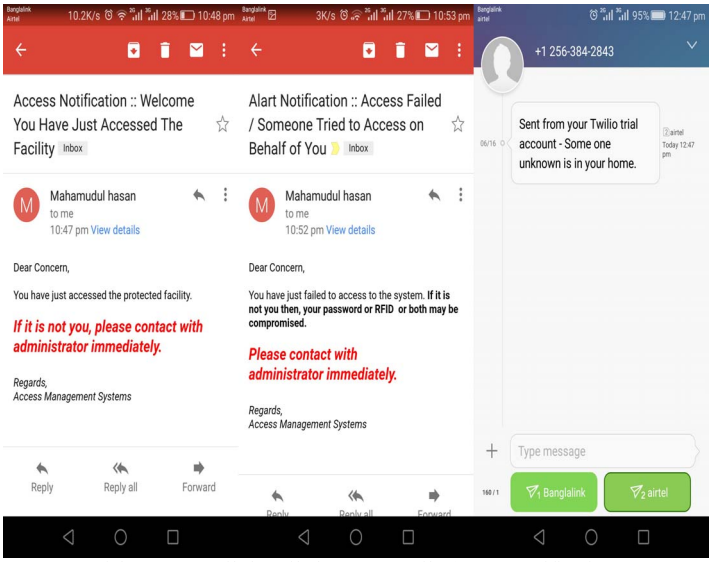
Performance analysis can be done in various ways. In this paper, performance is evaluated both qualitatively and quantitatively. These two analyses are described in the following subsections.

A. *Qualitative analysis:*

The qualitative analysis is done based on several parameters. These parameters are described in the following subsections.

a) Latency:

In real time embedded systems, latency is one of the key factors by which system's performance can be evaluated. The time interval between the application of input to the system and obtaining output from the system can be defined as system latency. There are three types of latencies in this system. They are Raspberry Pi 3 side system latency, IBM cloud server side latency and network side system latency. For simplicity, Raspberry Pi 3 side system latency and total system latency is measured since cloud side latency and network side latency are inconsistent over time. From the average of 50 instances, it is found that Raspberry Pi 3 side system latency is about 120ms in which the face recognition time is about 45ms as the total latency is about 3.5s.



(a) Successful access email (b)Failed access email (c) SMS notification

Fig. 5. E-mail and SMS based notification on mobile device

b) Data Security:

If the data of the system is stored properly and cannot be changed or altered, the security of the system is primarily ensured. The data is encrypted via AES 256 in system side and decrypted on server side. The key is being changed at a regular time interval to provide system integrity.

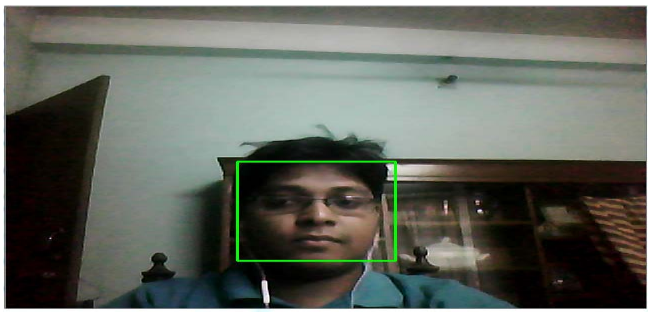


Fig. 6. Authorized face recognition

Fig. 7. Access management system

B. *Quantitaitve analysis:*

The quantitative analysis of the system is based on the performance of the back propagation of the neural network of the face recognition section. The following table shows the test data of three different samples. It is to be noted that each test is conducted 65 times. Every time true positive (TP), true negative (TN), false positive (FP) and false negative (FN) are calculated, and the recognition rate is denoted by the following equation.

$$RR = \frac{TP + TN}{TP + TN + FP + FN} \quad (6)$$

TABLE I. RECOGNITION RATE

	Test 1 $(\%RR)_{avg}$	*Test 2 $(\%RR)_{avg}$*	*Test 3 $(\%RR)_{avg}$*
Sample 1	83.31	81.32	85.11
Sample 2	85.32	82.71	87.31
Sample 3	84.74	81.57	89.74

For optimal performance of the face recognition system, the intensity of the light should be above 300 lux. All efficiencies (Test 1 and Test 2) of the table 1 are measured on 350 to 400 lux in daytime indoor condition. The system also recognizes the faces in day time outdoor environment(Test 3) where the light intensity is above 1000 lux.

Although it is tough to find homogeneous systems resembling the proposed system immaculately, the overall performance analysis of the access management system with some of the predecessor systems is shown in the following table.

TABLE II. PERFORMANCE ANALYSIS WITH RELEVENT SYSTEMS

Authors	*Latency*			*$(\%RR)_{avg}$*	
	System	*NN*	*Overall*	*Face*	*Others*
A. Derbel et al.[1]	N/A	N/A	N/A	**97.4%**	N/A
Y. Xin et al.[2]	N/A	N/A	N/A	**72.9%**	**70.4%(fingerprint) 68.2(palm vein)**
A. Mosenia et al.[3]	N/A	N/A	N/A	N/A	**91.1%(FRR) 91.8%(FAR)**
S.-H. Lee et al.[7]	N/A	N/A	N/A	**96.88%**	N/A
J.-J. Lin et al.[9]	N/A	N/A	N/A	**83%**	N/A
X. Peng et al.[10]	N/A	**3.6s**	**3.6s**	**92.9%**	N/A
F. Mahmud et al.[14]	N/A	N/A	N/A	**96.25%**	N/A
N. Xue et al. [15]	**0.6072s**	N/A	**.6074s**	N/A	N/A
Proposed work	**120ms**	**45ms**	**3.5s**	**89.74**	N/A

The cloud connectivity and integration of three layers of authentication in cost effective platform is unprecedented in the previously developed systems. Due to cost effective hardware and multistage authentication, the overall system latency is comparatively larger.

VI. COMPARATIVE ANALYSIS

The comparative analysis is accomplished based on comparing the developed system to some of the previously developed systems. The comparative analysis is shown in the TABLE III .

TABLE III. COMPARATIVE ANALYSIS WITH DIFFERENT SYSTEMS

Authors	*Password*	*RFID*	*Face recognition*	*IoT*	*Others*
A. Derbel et al.[1]	no	no	**yes**	no	**Gait**
Y. Xin et al.[2]	no	no	**yes**	no	**Finger print and palm vein**
A. Mosenia et al.[3]	no	no	no	no	**Bio signals**
L. Malina et al.[4]	no	**yes**	no	no	**Cryptography**
X. Wang et al.[6]	no	**yes**	no	no	No
S.-H. Lee et al.[7]	no	no	**yes**	no	no
PAN Xiang et al.[8]	no	**yes**	**yes**	no	no
J.-J. Lin et al.[9]	no	no	no	no	**NFC, digital signeture**
X. Peng et al.[10]	no	no	no	**yes**	no
M. Sahani et al.[11]	no	no	**yes**	no	**Zigbee GSM**
D. K. Sarker et al. [12]	**yes**	**yes**	**yes**	no	no
Proposed work	**yes**	**yes**	**yes**	**yes**	**SMS, Email, AES encryption**

In the proposed work, three layers namely, password, RFID and face recognition, based security system is developed and the IoT connectivity makes it easy for both the user and the administrator to verify the access. As the SMS and email are sent to user and administrator server, the access record is also preserved.

It is quite evident that most of the previously developed systems rarely concerned with more than two parameter access authentication and connectivity of those systems are seldom taken into consideration. Though some systems dealt with biosignals and zigbee based communication systems for ensuring systems data security, those systems showed seemingly complex method which will not only contribute to higher system latency but also will be prone to data taping if PAN ID of zigbee network is compromised or bio signal pattern is recognized via deep neural network. To prevent data tapping AES algorithm is employed in this work and the key is modified at a defined time interval which ensures data security.

In summary, few previously developed systems exploit three layers of hardware authentication, one layer of software based security for prevention of data tapping and three different connectivity schemes for access management system.

VII. CONCLUSION AND FUTURE WORKS

In this paper, three layer authentication based access management where data security is ensured via AES algorithm is developed. Implementation of three hidden layer back propagation based face recognition feature for both low light(indoor application) and day light(outdoor application) condition, which had recognition rate (RR) ranging from 81.32%(at low light) to 89.74%(at day light), improves the performance of the access management system. Incorporation of IoT environment for connectivity with AES algorithm for data security in software layer makes the system both flexible and secure simultaneously.

Presently, this system is using IBM's free IoT cloud server bluemix on trial basis which offers generic and limited development on their server. For dedicated smart

phone application stable api of the cloud server is required which is not available in this trial cloud platform. The free bluemix server also has limitations that prevent to employ good lossless data compression algorithm with fairly large blocks of code in server side. This free server also does not support over the air (OTA) update on remote devices. In future, when dedicated server for this access management system will be developed then, cloud connected smart phone application, exploitation of lossless data compression and OTA update on remote devices will be possible.

REFERENCES

[1] A. Derbel, D. Vivet and B. Emile, "Acess control based on gait analysis and face recognition", Electronics Letters, Vol. 51, No. 10, pp. 751–752, 14 May 2015

[2] Y. Xin, L. Kong, Z. Liu ,C. Wang, H. Zhu, M. Gao, C. Zhao, and X. Xu, "Multimodal Feature-Level Fusion for Biometrics Identification System on IoMT Platform" IEEE Access, vol. 6,pp. 21418 – 21426, 13 March 2018

[3] A. Mosenia, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "CABA: Continuous Authentication Based on BioAura" IEEE Transactions on Computers, Vol. 66, no. 5 , pp. 759 – 772, 27 October 2016

[4] L. Malina, V. Benes, J. Hajny, P. Dzurenda, "Efficient and Secure Access Control System Based on Programmable Smart Cards" in proc. of 40th IEEE International Conference on Telecommunications and Signal Processing (TSP), 5-7 July 2017,pp. 32-36

[5] C.C. Wu, C.-W. Hsu R.-S. Cheng"The digital signature technology for access control system of mobile" in proc. Of *IEEE International Conference on Applied System Innovation,* 13-17 April 2018 *pp.896-898*

[6] X. Wang, Y. Wang, " An office intelligent access control system based on RFID" in proc. Of *IEEE* Chinese Control And Decision Conference (CCDC), 9-11 June 2018,pp. 623-626

[7] S.-H. Lee, C.-S. Yang, "An Intelligent Home Access Control System Using Deep Neural Network" " in proc. Of *IEEE* International Conference on Consumer Electronics - Taiwan (ICCE-TW) 12-14 June 2017 *,pp. 281-282.*

[8] PAN Xiang "Research and implementation of Access Control System based on RFID and FNN Face Recognition" in proc. Of *IEEE* 2nd International Conference on Intelligent System Design and Engineering Application, 6-7 Jan. 2012, pp.716-719

[9] J.-J. Lin, S.-C. Huang "The Implementation of the Visitor Access Control System for the Senior Citizen Based on the LBP Face Recognition" in proc. Of *IEEE* International Conference on Fuzzy Theory and Its Applications (iFUZZY), 12-15 Nov. 2017 ,pp.1-6

[10] X. Peng, C. Van "Design of Access Control System Based on Stereo Face Recognition" in proc. Of IEEE International Conference on Computer Application and System Modeling (lCCASM 2010), 22-24 Oct. 2010,pp.557-561

[11] M. Sahani, C. Nanda, A. K. Sahu and B. Pattnaik "Web based online embedded door access control and home security system based on face recognition." in proc. Of IEEE International Conference on Circuit, Power and Computing Technologies, 19-20 March 2015 ,pp.1-6

[12] D. K. Sarker , N. I. Hossain , I. A. Jamil , "Design and implementation of smart attendance management system using multiple step authentication" in proc. Of IEEE International Workshop on Computational Intelligence (IWCI), 12-13 Dec. 2016, pp.91-95

[13] Vanlalhruaia , Y. K. Singh ; N. D. Singh "Binary face image recognition using logistic regression and neural network" in proc. Of IEEE International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS) , 1-2 Aug. 2017. ,pp. 3883-3888

[14] F. Mahmud , S. Afroge , M. A. Mamun , A. Matin "PCA and back-propagation neural network based face recognition system" in proc. Of IEEE18th International Conference on Computer and Information Technology (ICCIT), 21-23 Dec. 2015,pp. 582-587

[15] N. Xue, L.Liang, J. Zhang, X. Huang " An Access Control System for Intelligent Buildings"in proc of 9th EAI International Conference on Mobile Multimedia Communications, 18 - 20 June 2016 ,pp. 11-17

[16] "RDM 6300 datasheet " Seeed Studio, China.