A Multi-Modal Cloud-Assisted Authentication for Security in RFID Critical IoT Applications

Gouse Baig Mohammad [1], U Ravi Babu [2]

[1] Acharya Nagarjuna University, Guntur, Andhra Pradesh, India. Email: gousebaig@mjcollege.ac.in.
[2] Dr DRK College of Engineering and Technology, Hyderabad, Telangana, India. Email: uppu.ravibabu@gmail.com.

***Abstract* - Most of Radio Frequency Identification, RFID, critical applications follow RFID based authentication for security. In this paper we consider case studies such as Smart Home to investigate different scenarios that may occur in access control mechanism. Access to smart home is controlled by an authentication system using RFID based approaches in existing systems. Among the different possible scenarios in the access control mechanism, we concentrate on three: i) the first one is the case in which an authorized person carries authorized RFID tag to enter into a smart home, ii) the second case is that an unauthorized person carries an authorized RFID tag (probably stolen RFID tag), and iii) the third case is that an unauthorized person carries an unauthorized RFID tag.**

Keywords* - *RFID (Radio Frequency Identification Device), Authenticated Cloud Server (ACS)

I. INTRODUCTION

Authentication is one of the security approaches to safeguard systems. From the literature [26], [27] and [28], it understood that most of the RFID critical applications followed RFID based authentication for security. Considering the case study such as SMART HOME in this paper, we investigated further and came to know different scenarios that may occur in access control mechanism of this use case. Access to smart home to humans is controlled by an authentication system using RFID based approaches in existing systems. Figure 1 shows different scenarios that may be possible in the access control mechanism. There are three scenarios out of which the first one is the case in which an authorized person carries authorized RFID tag to enter into smart home. The second case is that an unauthorized person carries an authorized RFID tag (probably stolen RFID tag). The third case is that an unauthorized person carries an unauthorized RFID tag.

II. LITERATURE REVIEW AND WEAKNESS OF CURRENT TECHNIQUES

In the first scenario, the person needs to be allowed into smart home. In the second and third cases, it is essential to have control mechanism or efficient scheme to ensure that the authentication is not successful due to obvious reasons aforementioned. In case 2, the person is not actually an authorized person but he carries authorized RFID tag. In such cases, all the authentication systems that given importance to only valid RFID tag will fail to prevent the person in entering smart home. Therefore, a more efficient mechanism is essential to deal with it. In the third case, the person is not authorized and the RFID tag is also not authorized one. This is the very obvious case where the system needs to reject entry to the person. Out of the three cases, the second case throws litmus test to any authentication systems that prevail in RFID critical applications.

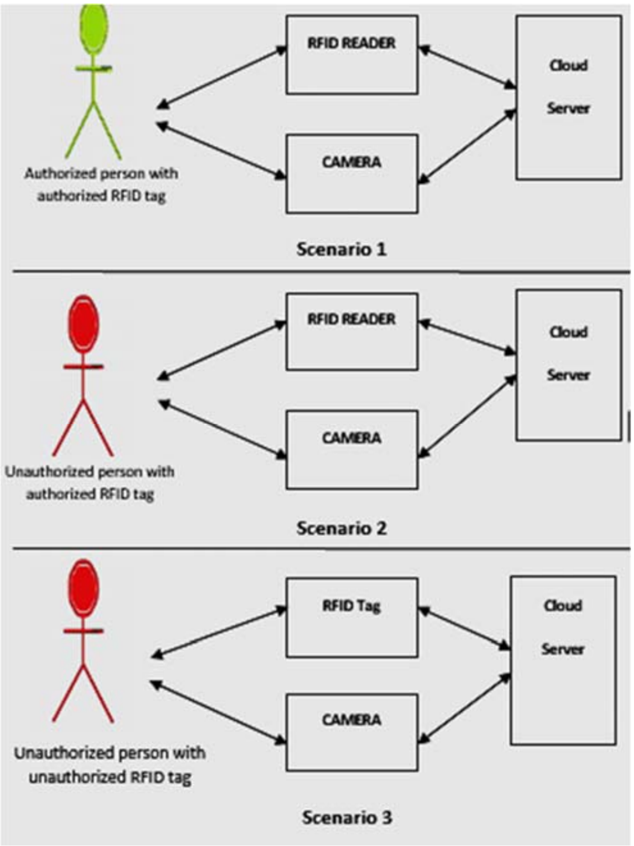
RFID READER
Cloud Server
CAMERA
Authorized person with authorized RFID tag
Scenario 1
RFID READER
Cloud Server
CAMERA
Unauthorized person with authorized RFID tag
Scenario 2
RFID Tag
Cloud Server
CAMERA
Unauthorized person with unauthorized RFID tag
Scenario 3

Figure 1: Different authentication scenarios and security issues.

III. PROPOSED NEW TECHNIQUE

This section describes the system model considered for the proposed methodology. It provides an architectural overview of the scenario in which RFID tags, RFID readers and other readers involved in authentication process. Authenticated Cloud Server (ACS) and backend server play an important role while all communicating parties have their own role to play in the process. Figure 2 shows the overview of the system model.

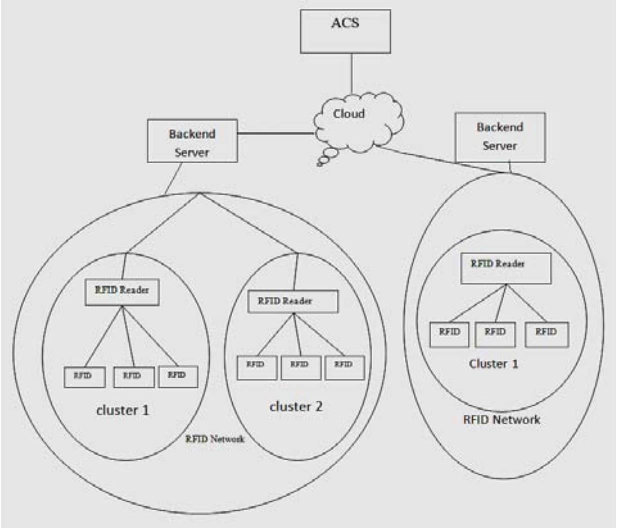

Figure 2: Shows the overview of the system model.

RFID tags with corresponding RFID readers form a cluster. There might be number of clusters found in the RFID network. And there might be number of RFID networks as well. There is communication among nodes within a cluster and also inter-cluster communication is possible. There might be communication between two different RFID networks as well which is to be coordinated by ACS. RFID tag is an entity in the model which carries identity information. According to the use case SMART HOME, the tag is carried by humans. The tag information may include shared key, sequence number, emergency security keys and id of server. Once RFID tag is registered with the server, RFID computes one time alias and location identifier v1 of the tag reader.

Tag reader on the hand contains credentials such as server id, track sequence number, one time alias identifier, and location information. It works as the mediator between RFID tag and backend server. It reads tag information and sends the same to backend server. Reader also gets its security credentials from backend server. Security information and the information of the networks are stored in backend server. It provides shared keys to all parties. It also has emergency keys to be used as and when required. In fact it has security credentials of tag readers and tags.

ACS on the other hand is used to group different RFID networks together. It coordinates communication between two RFID networks. In this case, it helps in sending data from one cluster of a network to another cluster of different network. For this to work well, every backend server details are known to ACS. The role of backend server is to ensure communication between clusters of same network. Nodes within a cluster and between two clusters can have communication through backend server.

IV. PROPOSED AUTHENTICATION PROCESS-SIMULATION METHOD

The authentication process is twofold. The smart home use case needs secure authentication without causing the case 2 and case 3 described in Section 3 to succeed. This section presents the proposed authentication process followed by detailed communications in authentication scheme among different parties involved. Initially an authorized user's image is captured and stored in cloud server along with his/her RFID tag reference. This phase is called reference registration. Once reference registration is completed, it will be tag information an image data are associated with the persona and saved in public cloud. After this, when any person arrives at the smart home, the system captures his image live and readers RFID tag information. Then the flow of the proposed authentication is as in Figure 3.

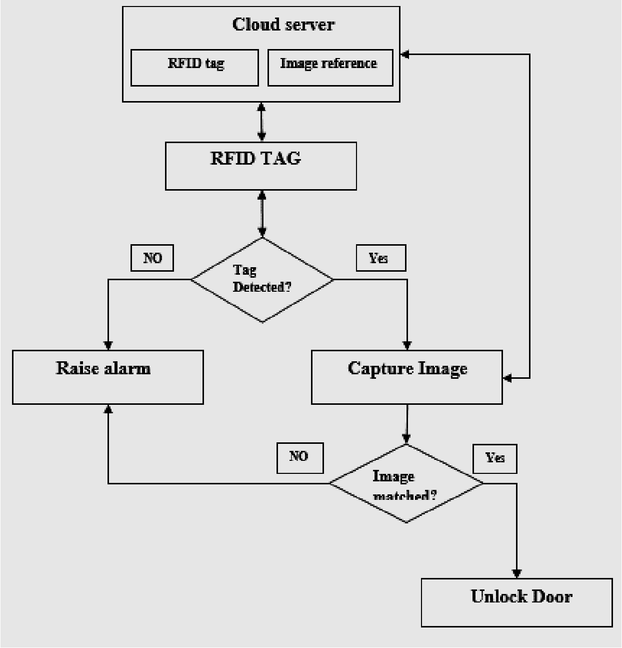

Figure 3: Overview of the proposed multi-modal authentication system for smart home.

When a person is to be authenticated securely, the RFID reader reads tag information. Tag information contains identity of the person with respect to smart home use case. The system forwards the tag information and sends it to server for RFID based authentication. If the RFID tag information matches with corresponding tag information in the reference registrations data, the first modal of authentication is successful. If not successful, the system declares the person as unauthorized and raises alarm. In case of successful RFID authentication, the system initiates the second model of authentication. In this model, the system captures image of the person and matches with the corresponding reference registration images stored in public cloud. If the image is matching then, the person is declared as authenticated person and allowed to gain access to smart home.

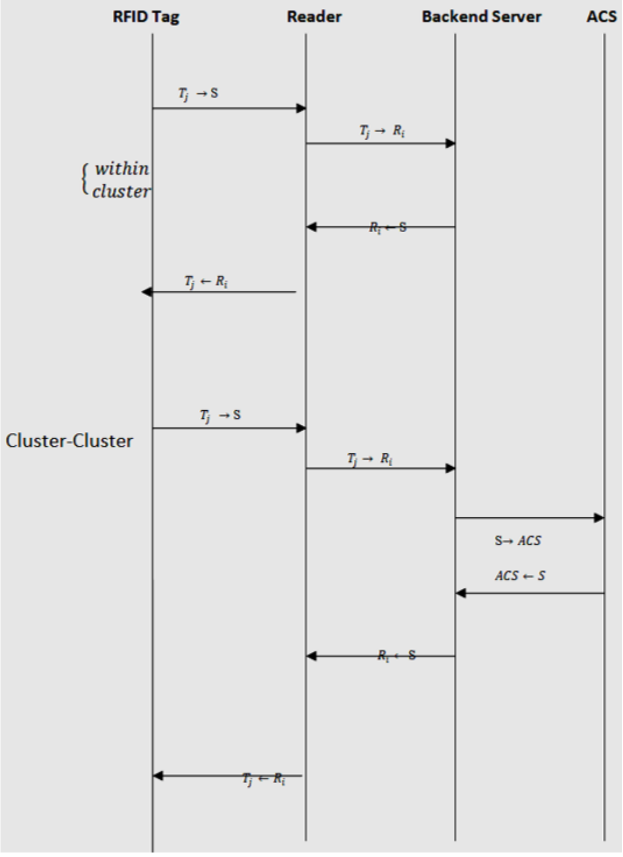

Figure 4: Overview of the proposed scheme

A. *Multi-Modal Authentication-Communication Among Parties*

Communication is possible within the network and between two networks. When communication takes place in the same network it is as follows:

A1. In Same Network: When RFID tag needs interaction with the reader and the reader needs to interact with backend server it can be done in this fashion.

First RFID tag sends its credentials (server id, one time alias identifier, track sequence number, location, V_1) to reader and then reader sends tag details along with its details (location, V_2) also to backend server. Afterwards, server checks the details with the help of track sequence number. If track sequence number is not valid it uses emergency keys to identify the tag. Then server provides security credentials to reader and tag.

A2. Communication with Another Network: In order to transfer credentials from one network to another network two backend servers are to register with each other. The presence of ACS can help them to have communication between two networks. ACS is thus important entity that is useful only in the case of inter-network communications. RFID tag communicates with reader and then reader can communicate with backend server. Afterwards, the backend server communicates with the ACS to get details of another network's backend data base server. ACS is only source to get details of another network backend data base server. After getting credentials from ACS, server sends to reader, reader sends these credentials to RFID tag. Then tag communicates with another network and start data transmission.

B. Image Matching

With respect to Figure 2, the image matching is carried out in this paper as presented in Figure 3. The image matching part of the proposed algorithm is inspired by the work of [29]. The novelty of the proposed matching is that it makes use of DAISY descriptor which showed better performance when compared that of SURF and SIFT feature descriptors.

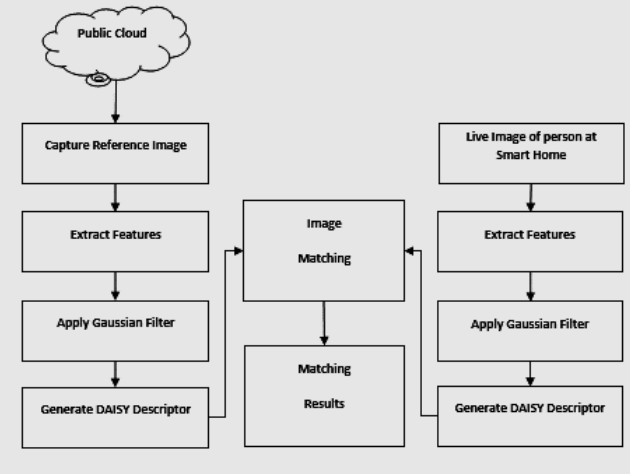

Figure 5: Flowchart of image matching.

As mentioned earlier, after successful RFID tag authentication, live image of the person who seeks entrance into smart home is captured by camera and the same is sent to cloud server for authentication. The matching procedure involves creation of DAISY descriptor for both the live image of the person and the corresponding image associated with the RFID tag information. Given image is subjected to feature point detection or feature extraction. In order to achieve this, a matrix known as Hessian matrix is computed as follows.

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

Here L represents convolution of the image. It is also known as Gaussian's second derivative. A determinant is then computed to speed up the process of matching. It is as follows.

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

Once feature points are detected and determinant is computed, Gaussian filter is employed to capture patterns. Then, from the image DAISY descriptor is generated as follows.

$$\bar{x} = \frac{\partial^2 H^{-1}}{\partial^2 x}\frac{\partial H}{\partial x} \tag{3}$$

After getting DAISY descriptor, representative points and sample points are computed a follows.

$$Dx(X_i) = I(X_i^1) - I(X_i^5) \tag{4}$$

$$Dy(X_i) = I(X_i^3) - I(X_i^7) \tag{5}$$

This procedure is carried out for reference image obtained from public cloud and the live matching image of the person who sought entry into smart home. The DAISY descriptors of both the images are matched. The matching results either positively or negatively. If the matching is correct or positive, then the multi-modal authentication procedure is successfully completed. If the matching is not successful, the system notifies people concerned and raises an alarm. The door remains locked.

V. SIMULATION AND RESULTS

Experiments are made with NS2 platform which is widely used for communication networks. With respect to image authentication, an image dataset is collected from [30]. This dataset is provided by AT&T and Cambridge University Computer Laboratory (CUCL). The dataset has actually 40 subjects with 10 images per subject. Each image is different from other images in terms of facial expressions, time at which it is captured and the lighting conditions.. Images are of 256 gray level per pixel and of size 92x112.

An excerpt of 8 subjects with 10 images each (variants of a single person). The reason behind choosing this dataset is that it provides different variation in the images of same person which closely matches to the needs of smart home case study. As the images are captured at different times with different lighting conditions and facial expressions, they are suitable for evaluating the proposed authentication scheme. The results of the proposed system are compared with state of the art authentication schemes found in the literature. They are known as Broadcast Authentication (BA), Certificate Based Authentication (CAS) and the other scheme named Direct Storage Based Authentication (DAS). More information on these schemes is available in [31]. Moreover, with respect to DAISY descriptor used for image matching, the results are compared with other state of the art descriptors known as SIFT and SURF. Figure 6 shows simulation environment used in NS2.

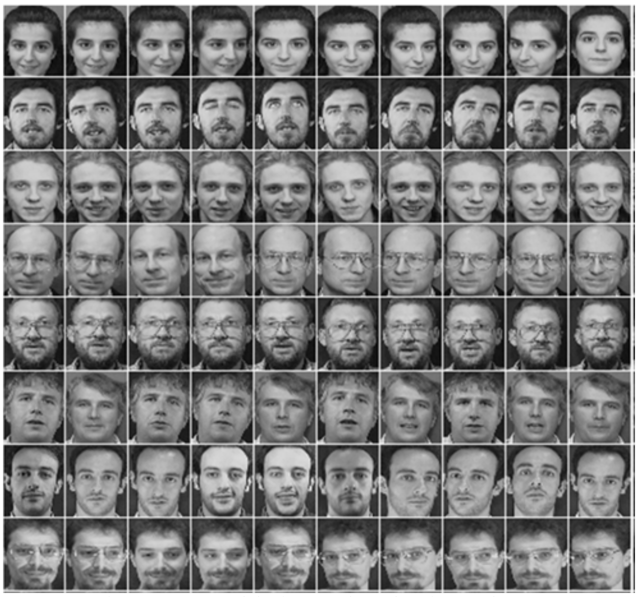

Figure 6. Some of the images from face image dataset

TABLE I. SIMULATION ENVIRONMENT USED

Parameter	Value
channel type	Channel/WirelessChannel
radio-propagation model	Propagation/TwoRayGround
network interface type	Phy/WirelessPhy
MAC type	Mac/802_11
interface queue type	Queue/DropTail/PriQueue
link layer type	LL
antenna model	Antenna/OmniAntenn
max packet in ifq	100
number of mobile nodes	29
routing protocol	AODV
X dimension of topography	1000
Y dimension of topography	1000

TABLE II. PACKET DELIVERY

Simulation Time (Sec)	Packet Delivery (%)			
	CAS	DAS	BA	Proposed
100	3	5	7	9
200	7	10	13	23
300	13	19	25	31
400	21	27	34	42
500	30	36	42	52
600	36	43	52	63
700	44	50	60	74
800	56	61	69	82
900	62	70	78	90
1000	64	80	88	94

The simulation environment is used for the proposed system model. The implementation of the proposed model is evaluated with simulation study. The results are as follows. Table II indicates the packet delivery rate and the corresponding graph is depicted by Fig. 7.

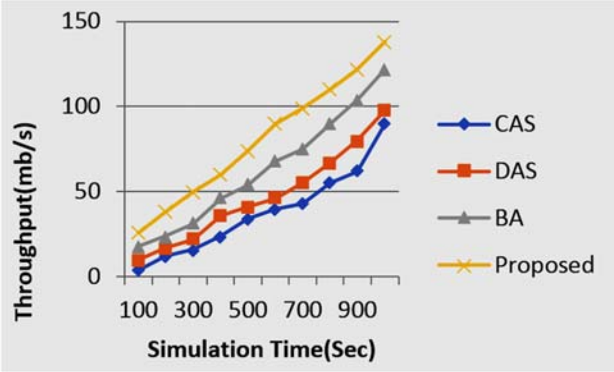

Figure 7. Graph showing Packet Delivery

Table III indicates the packet dropping rate and the corresponding graph is depicted by Fig. 8.

TABLE III. PACKET DELIVERY

Simulation Time(Sec)	Packet Dropping(%)			
	CAS	DAS	BA	Proposed
100	32	26	22	18
200	40	34	29	23
300	45	39	34	28
400	54	48	41	33
500	60	51	45	40
600	70	64	57	51
700	75	70	67	60
800	88	80	73	65
900	92	86	77	70
1000	96	92	82	75

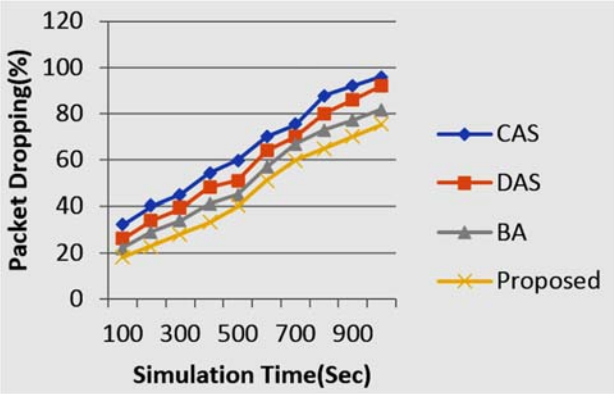

Figure 8. Graph showing Packet Drop

Table IV-A indicates the Energy in joules and the corresponding graph is depicted by Fig. 8.

TABLE IV-A. ENERGY

Simulation Time(Sec)	Energy(Joules)			
	CAS	DAS	BA	Proposed
100	2500	280	850	450
200	3600	600	1300	700
300	4600	900	1600	1100
400	6200	1300	2100	1500
500	7300	1900	2900	2200
600	8200	2500	3600	2900
700	9700	2900	4100	3300
800	9980	3200	4500	3800
900	9990	3600	6200	4300
1000	9990	4800	8200	5400

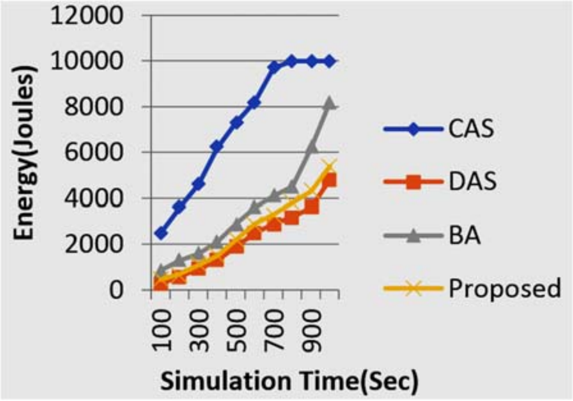

Figure 9. Graph showing Packet Drop

TABLE IV-B. 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	88.54	38.12	73.54	81.23	88.65	75.62

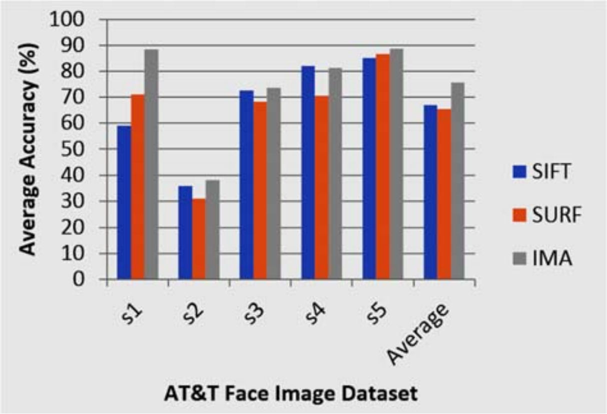

Figure 10. Average accuracy (%) of matching with different subjects of AT&T dataset.

Table V represents the Average execution time (sec) for matching with different subjects of AT&T dataset and Figure 11 represents the corresponding graph.

TABLE V. AVERAGE EXECUTION TIME (SEC) FOR MATCHING WITH DIFFERENT SUBJECTS OF AT&T DATASET

Algorithms	Average Accuracy (%)					
	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	12.58	14.35	19.54	11.08	12.96	16.58

Table VI and Figure 12 show the Precision & Recall values of SIFT, SURF and Proposed methods. Table 7 and Figure 13 represents the Average accuracy of matching with different subjects of AT&T dataset. Table 8 & Figure 14 represents the Average execution time (sec) for matching with different subjects of AT&T dataset.

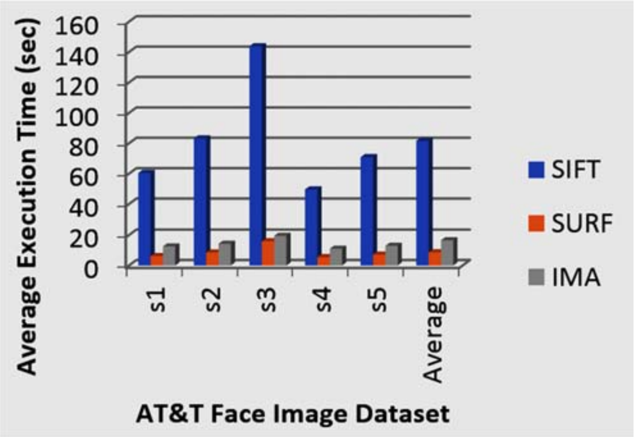

Figure 11. Average execution time (sec) for matching with different subjects of AT&T dataset.

TABLE VI. PRECISION & RECALL

	Precision	Recall
SIFT	90	7.5
SURF	83	20.56
PROPOSED	98	12.43

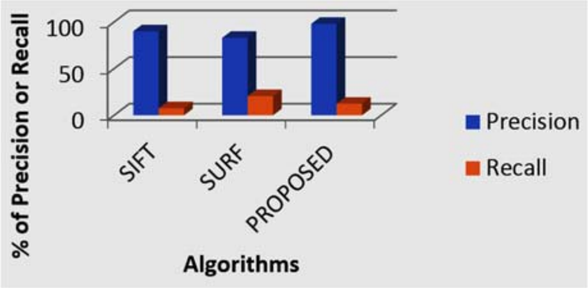

Figure 12. Precision & Recall

TABLE VII. AVERAGE ACCURACY (%) OF MATCHING WITH DIFFERENT SUBJECTS OF AT&T FACE IMAGE 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	88.54	38.12	73.54	81.23	88.65	75.62

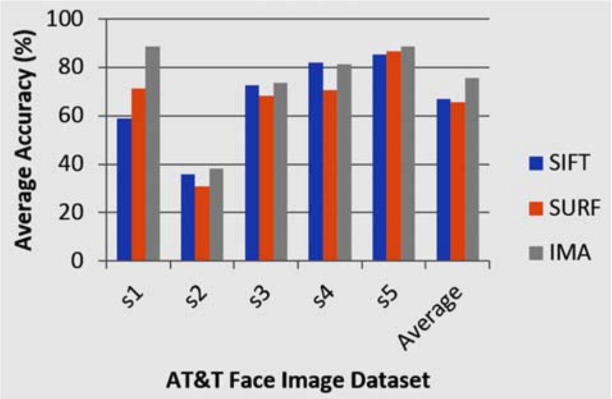

Figure 13. Average accuracy (%) of matching with different subjects of AT&T dataset.

TABLE VIII. AVERAGE EXECUTION TIME (SEC) FOR MATCHING WITH DIFFERENT SUBJECTS OF AT&T DATASET

Algorithms	Average Accuracy (%)					
	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	12.58	14.35	19.54	11.08	12.96	16.58

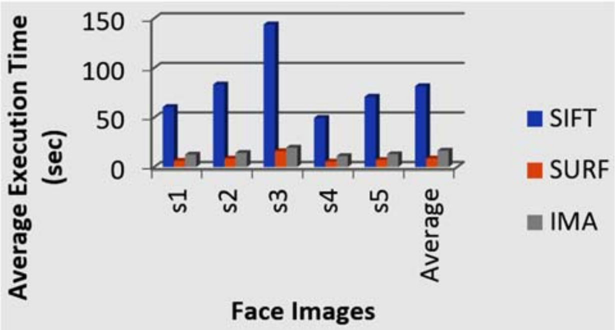

Figure 14 Average execution time (sec) for matching with Face Images.

VI. CONCLUSION

The images are in .PGM format and EvalVid toolkit is used to convert images into traces in order to complete experiments in NS2 for image matching part of the proposed authentication scheme and the results are very satisfactory. A better algorithm can be designed with different data sets,a better security is being provided this processes as It coordinates communication between two RFID networks. in this paper, we investigated further and came to know different scenarios that may occur in access control mechanism of this use case.

REFERENCES

[1] Pardeep Kumar,An Brae.ken, Andrei Gurtov,Jari Iinatti,and Phuong Hoai Ha. (2017). Anonymous Secure Framework in Connected Smart Home Environments. IEEE Transactions On Information Forensics And Security. 12 (4), p1-13.

[2] Leandro Y. Manoa,Bruno S. Faic¸ala, Luis H. V. Nakamuraa,b, Pedro H. Gomese, Giampaolo L. Libralonc, Rodolfo I. Meneguete b, Geraldo P. R. Filhoa, Gabriel T. Giancristofaroa, Gustavo Pessind, Bhaskar K. (2016). Exploiting IoT technologies for enhancing Health Smart Homes through patient identification and emotion recognition. IEEE, P1-15.

[3] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. (2016). On Privacy and Security Challenges in Smart Connected Homes. European Intelligence and Security Informatics Conference, p1-4.

[4] Shancang Li, Li Da Xu, Shanshan Zhao. (2018). 5G Internet of Things: A Survey. Journal of Industrial Information Integration, p1-29.

[5] Mattias T. Gebrie and Habtamu Abie. (2017). Risk-Based Adaptive Authentication for Internet of Things in Smart Home eHealth. ACM, p1-7.

[6] Marianthi Theoharidou, Nikos Tsalis, and Dimitris Gritzalis. (2016). Smart Home Solutions for Healthcare: Privacy in Ubiquitous Computing Infrastructures. IEEE, P1-10.

[7] Faheem Zafari,Ioannis Papapanagiotou,and Konstantinos Christidis. (2017). Micro-location for Internet of Things equipped Smart Buildings. IEEE, p1-16.

[8] Muhammad Raisul Alam,M. B. I. Reaz and and M. A. Mohd Ali. (2012). A Review of smart Homes past ,present, future. IEEE, p1-16.

[9] Andreas Kamilaris and Andreas Pitsillides. (2015). Social Networking of the Smart Home. IEEE, p1-6.

[10] Min Chen,Jiafu Wan,Jiafu Wan,Xiaofei Liao,and Victor C.M. Leung. (2013). A Survey of Recent Developments in Home M2M Networks. IEEE Communications Surveys & Tutorials. 16 (1), P1-17.

[11] Andreas Jacobsson and Martin Boldt and Bengt Carlsson. (2010). On the Risk Exposure of Smart Home Automation Systems. IEEE, p1-8.

[12] Rosslin John Robles1 and Tai-hoon Kim1. (2010). A Review on Security in Smart Home Development. International Journal of Advanced Science and Technology. 15 , P1-10.

[13] Ji Eun Kim1,3, George Boulos3, John Yackovich3, Tassilo Barth4, Christian Beckel2, Daniel Mosse3. (2012). Seamless Integration of Heterogeneous Devices and Access Control in Smart Homes. IEEE, p1-8.

[14] Alessio Botta, Walter de Donato, Valerio Persico, Antonio Pescap. (2014). On the Integration of Cloud Computing and Internet of Things. IEEE, p1-8.

[15] Matthias Kovatsch, Markus Weiss, Dominique Guinard. (2017). Embedding Internet Technology for Home Automation. IEEE, p1-8.

[16] Michael E. Porter and James E. Heppelmann. (2014). How Smart, Connected Products Are Transforming Competition. Spotlight On Managing The Internet Of Things, p1-23.

[17] Andreas Jacobsson and Paul Davidsson. (2015). Towards a Model of Privacy and Security for Smart Homes. IEEE, p1-7.

[18] Mike Blackstock and Rodger Lea. (2014). IoT Interoperability: A Hub-based Approach. IEEE, p1-6.

[19] Miguel A. Zamora-Izquierdo, José Santa and Antonio F. Gómez-Skarmeta. (2010). Integral and Networked Home Automation Solution towards Indoor Ambient Intelligence. IEEE, p1-11.

[20] Terence. K. L. Huia, R. Simon Sherratta, DanielDıaz Sanchezb. (2017). Major Requirements for Building Smart Homes in Smart Cities based on Internet of Things Technologies. Preprint submitted to Special Issue on Smart City and Internet of Things, p1-20.

[21] Earlence Fernandes,Jaeyeon Jung and Atul Prakash. (2016). Security Analysis of Emerging Smart Home Applications. IEEE Symposium on Security and Privacy, p1-19.

[22] Andreas Jacobssona, Martin Boldtb, and Bengt Carlssonb. (2010). A Risk Analysis of a Smart Home Automation System. IEEE, p1-19.

[23] Jordi Mongay Batalla,Athanasios Vasilakos And Mariusz Gajewski. (2017). Secure Smart Homes: Opportunities and Challenges. ACM Computing Surveys. 50 (5), p1-32.

[24] Christos Stergiou , Kostas E. Psannis , Byung-Gyu Kimb, Brij Guptac. (2018). Secure integration of IoT and Cloud Computing. Future Generation Computer Systems. 78 , p964–975.

[25] Mung Chiang and Tao Zhang. (2016). Fog and IoT: An Overview of Research Opportunities. IEEE Internet Of Things Journal. 3 (6), p1-11.

[26] Jung Tae Kim. (2014). Authentication Process between RFID tag and Mobile Agent Under U-healthcare System. International Journal of Bio-Science and Bio-Technology. 6 (3), p109-116.

[27] Prosanta Gope , Ruhul Amin , S.K. Hafizul Islam ,Neeraj Kumar and Vinod Kumar Bhalla. (2017). Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. *Future Generation* Computer Systems, p1-10.

[28] S. A. Ahson. and M. Ilyas. (2017). “RFID handbook: applications, technology, security, and privacy”. CRC press.

[29] Li, L. (2014). Image Matching Algorithm based on Feature-Point and DAISY Descriptor. Journal of Multimedia, 9 (10), p829-834.

[30] Andy Hopper FREng. (2002). Cambridge University Computer Laboratory. AT&T Laboratories Cambridge. Retrieved http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html

[31] Hamzeh Ghasemzadeh, Mohammad Reza Aref and Ali Payandeh (2013). A novel and low-energy PKC-based key agreement protocol for WSNs.