May – June 2020
ISSN: 0193-4120 Page No. 9461 - 9469

RFID and Biometric Authentication Framework for Secure Access to IoT based Smart Home

K. S.Niraja, Research Scholar,C.S.E, K.L.E.F,Vaddeswaram, Guntur, AP, India,
Dr.Sabbineni Srinivasa Rao,Associate Professor,C.S.E, K.L.E.F,Vaddeswaram, Guntur,AP, India

Article Info
Volume 83
Page Number: 9461 – 9469
Publication Issue:
May - June 2020

Article History
Article Received*: 19 November 2019*
Revised*: 27 January 2020*
Accepted*: 24 February 2020*
Publication*: 18 May 2020*

Abstract:
Internet of Things (IoT) emerged as the combination of different technologies that brought about many uses cases such as smart home, smart healthcare and smart transportation to mention few. All these IoT applications are realized wit Machine to Machine (M2M) interactions minimizing human intervention. Radio Frequency Identification (RFID) is the technology which is essential to realize IoT applications. RFID is used for identification of objects and also used for authentication purposes. On the contrary to barcode, RFID eliminates issues like line of sight and distance. RFID tags may carry sensitive data as well. Therefore, it is essential to safeguard communications where RFID is involved. In this paper smart home IoT use case is considered for empirical study. A security framework is proposed to ensure cloud based authentication that involves both RFID and biometric. The framework is implemented to ensure end to end security and privacy in smart home application scenario. The experimental results revealed that the proposed framework performs better than the state of the art.

Keywords*: Internet of Things (IoT), smart home, security, privacy, biometric authentication*

Introduction:

Radio Frequency Identification (RFID) is the technology that is used to track objects in IoT use cases. It can uniquely identify objects and overcomes the issues such as light of sight and distance that are exhibited by its predecessor barcode. It is widely used in smart buildings, smart cities and smart inventory management to mention few [1]. RFID is widely used in many real world applications. RFID tag is used in smart homes for authentication purposes. To realize IoT use cases, RFID and sensor networks are essential [4]. RFID is widely used in IoT integrated applications as studied in [8], [9], [14], [16], [17]- [20]. There are many smart IoT use cases where RFID is practically implemented. Some of them include smart city, smart transportation system, monitoring building occupancy, smart healthcare and so on.

Since RFID tag carries identification information and other sensitive information such as location of user, there is probability for privacy issues. The exchange of information between tag and tag reader and other parties in the smart home case study needs to be secured from different kinds of attacks. Data leakage is one of the problems in IoT integrated applications. In all location based services, there is possibility of privacy attacks. Therefore, there is need for protecting identity of users and also their queries in the IoT applications [5]. Many researchers in [4], [10], [12], and [15] contributed to address privacy concerns associated with RFID based authentication.

From the literature, it is understood that many IoT based smart applications used RFID for authentication and also object identification. IoT is realized by the combination of many technologies that are cross-disciplinary including sensing technologies, RFID, and telecommunications. RFID became very important technology for IoT use cases. However, there are security and privacy issues when RFID is used for authentication process and identity based communications. The rationale behind this is that RFID tags carry identify information that is associated with security and they also carry sensitive

May – June 2020
ISSN: 0193-4120 Page No. 9461 - 9469

information that causes privacy issues. Therefore, ensuring privacy and security in RFID based IoT use cases is an open problem considered. When this problem is solved, it paves way for increased usage of IoT applications in the real world. This is the motivation behind this research. Our contributions in this paper are as follows.

- Secure Access Control Scheme (SACS) is proposed for IoT integrated smart home case study. It has many features such as secure localization, mutual authentication, scalability, availability, strong anonymity and forward secrecy.
- Both RFID and biometric based authentication schemes are integrated to have higher level of security.
- Python data science platform is used to implement a prototype application. The results showed the utility of the biometric feature along with RFID based authentication process.

The rest of the paper has different sections to provide more details. Section 2 provides literature review related to IoT integrated authentication schemes. Section 3 provides biometric and RFID authentication scheme. Section 4 improves it further with privacy preserving approach. Section 5 presents results of empirical study. Section 6 provides conclusions drawn and gives ideas for future scope of the work.

2. RELATED WORK

This section covers literature review on RFID based and other authentication schemes in IoT integrated applications. Gope *et al*. [1] proposed RFID based scheme for authentication for smart city use case. Different security features like anonymity, authentication, forward secrecy and secure localization are explored. They opined that the location information needs to be safeguarded. Akkaya *et al*. [2] focused on the tracking and localization of people. They incorporated fusion techniques and used occupancy monitoring as well. Hernandez-Ramos *et al*. [3] proposed a security scheme named SAFIR for smart home use case. It has distributed approach with sensing and identification of objects besides data dynamics for gaining intelligence.

Importance of RFID in realizing smart cities is explored in [8]. Arjunan et el. [9] studied RFID based access control with energy efficiency to smart buildings case study. They found that RFID tags that are theft or misplaced lead to security breaches. This kind of research made in [14] also revealed the leakage of sensitive information. Das *et al*. [16] on the other hand tried different models for estimating the level of security in smart buildings. In the same fashion, in [17] protecting user location information from privacy attacks is given importance. In [18] smart environments are focused with respect to integration of hardware and software. Challa *et al*. [19] on the other hand investigated on the present authentication mechanisms being used in IoT use cases while in [20] RFID and its applications in IoT use cases is given importance.

Other researchers [21], [22], [23] and [24][26][27] also found the importance of RFID. In IoT applications, there is Machine to Machine (M2M) communication and also pervasive computing prevailed. When RFID is used for authentication in such applications, there are possible security issues like misusing RFID tag. Ziegeldorf *et al*. [4] specified that RFID plays vital role in realizing IoT. However, it is found to be vulnerable when secure communications are not established. Thus security and privacy are essential for safeguarding IoT applications. The privacy related issues are studied in [5] with respect to vulnerabilities and privacy related threats. Zhang *et al*. [6] investigated privacy and security issues pertaining to smart city application where smart home applications can exist. They found leakage of sensitive data may occur due to heterogeneous devices and standards. User privacy with respect to RFID critical applications is investigated in [7] and proposed a framework known

May – June 2020
ISSN: 0193-4120 Page No. 9461 - 9469

as SeCoMan to protect the system from privacy issues.

Mehrotra *et al*. [10] found that there are privacy challenges when RFID is used in IoT applications. They advocated privacy aware approaches for such applications. Kuzlu *et al*. [11] opined that there are different wireless technologies that paly their role in IoT applications along with RFID. They include Wave2M, IEEE 802.15.3a, Bluetooth and so on. Chen *et al*. [12] opined that location information in sensitive in nature. Liang *et al*. [13] on the other hand investigated on Advanced Persistent Threat (APT) with respect to cloud infrastructure. Cusack and Khaleghparast [15] reviews on the privacy gaps in IoT projects. From the literature, it is known that there is need for secure end to end communications with privacy as well. Towards this end both biometric and RFID based security is proposed in this paper.

3. NEED FOR RFID AND BIOMETRIC AUTHENTICATION FRAMEWORK

This section focuses on biometric and RFID based scheme and its need in protecting communications in smart IoT applications. In the system model used for authentication there many components involved. They include RFID reader for reading data from RFID tag, GSM modem, server, micro controller besides the locks and alarms. RFID tags preferred for empirical study are semi-passive in nature. The reason behind this is that such tags have ability to use power obtained from radio waves and battery. When a human carries RFID tag, it is read by reader nearby while camera is capture face of human live for biometric authentication process.

As a person nears smart home with the intention to enter the home, RFID reader and camera work to capture identity information. The data is sent to server in cloud where the both authentication data are verified. The procedure for verification is illustrated in Figure 1. The door of smart home is opened automatically when the authentication is successful. If not alarm raises and the locks remain closed. There will be notifications sent to all stakeholders of the application.

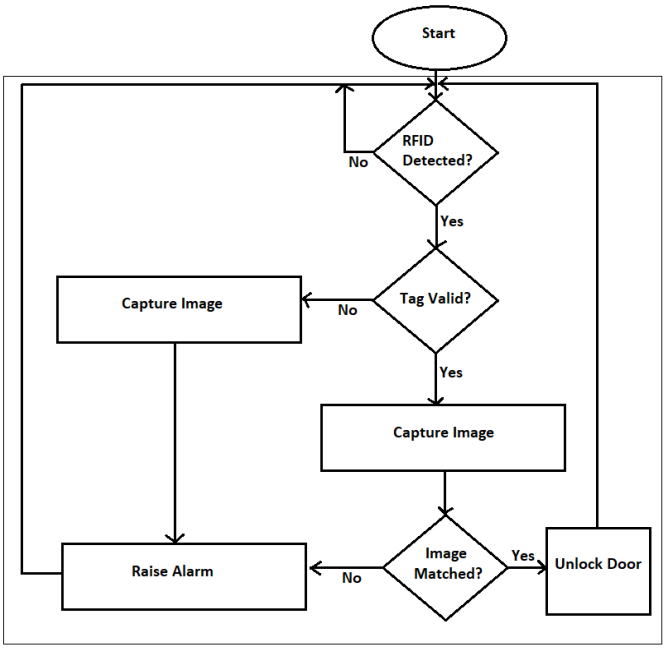

Figure 1: Biometric and RFID based authentication procedure

As presented in Figure 1, it is understood that both RFID tag information and human face are captured by RFID reader and camera respectively. First, RFID tag is verified. If the RFID tag is wrong, then system raises alarm and authentication process fails. If RFID based authentication is found to be successful, then the second layer of authentication that is biometric authentication takes place. If the biometric authentication succeeds, the door will get opened. If not, the door remained closed and notification is sent to stakeholders besides raising alarm.

3.1 Drawbacks of RFID Based Authentication

RFID based scheme has severe drawback. When RFID based authentication is followed in case of smart home for allowing access, there are possibilities to use stolen RFID tags. As the stolen RFID tags enable successful authentication of unauthorized tag holder, it has security lapses. When RFID tags carry sensitive information, there are privacy issues as well. In the proposed scheme, to overcome these drawbacks, biometric authentication is used along with RFID based authentication for higher level of security.

May – June 2020
ISSN: 0193-4120 Page No. 9461 - 9469

4. SECURE ACCESS CONTROL SCHEME (SACS)

4.1 Problem Definition

RFID based schemes used for authentication exhibited limitations. The rationale behind this is that RFID tags may be stolen by adversaries. Or the tags may be subjected to forgery attacks. As RFID tags carry location information, it leads to privacy issues. There is heavy computational complexity in the RFID based schemes used for authentication in the wake of constrained computing capabilities of RFID tags. This may cause potential risk to RFID based schemes. In addition to this most of the schemes that existed based on RFID are not suitable for IoT use cases like smart homes. This is the problem addressed in this paper.

4.2 Proposed Scheme

We proposed a scheme known as Secure Access Control Scheme (SACS). This scheme not only provides secure end to end communications but also preserve privacy. When the tag information is exchanged, its data privacy is ensured. The notations used in this scheme are provided in Table 1.

Notation	Description
T_j	j[th] tag
R_i	i[th] tag reader
S	Denotes backend server
ID_{T_j}	Reflects $T_j's$ identity
AID_T	Reflects $T_j's$ alias identity
PID	$T_j's$ pseudo identity
S_{id}	Represents identity of S
N_t	Represents random number
N_r	Represents another random number
K_{ts}	It denotes key shared between S and T_j
K_{em}	It denotes emergency key shared between S and T_j
K_{rs}	It denotes secret key shared between S and R_i
Tr_{seq}	It denotes sequence number tracked
LAI	Denotes identification of location area
h(•)	Denotes has function (one-way)
$\oplus$	XOR
$\|\|$	Concatenation

Table 1: Symbols and their meaning

Both RFID tags and readers are registered with backend server. Security keys are provided to them by backend server. Similarly, backend server is registered with Authenticated Cloud Service (ACS) which facilitates communication between two RFID networks. In other words, ACS makes communication possible between any two backend servers. The secure communication process among these three parties is illustrated in Figure 2.

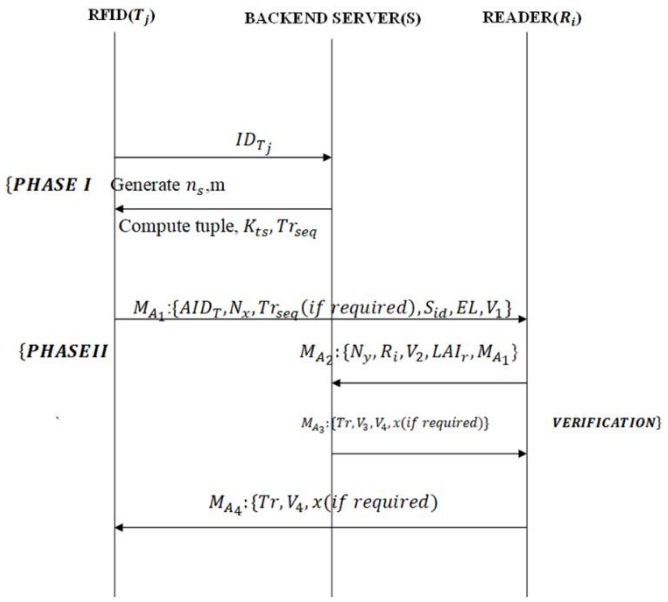

Figure 2: RFID based authentication with security and privacy preserved

In the SACS, there are two phases such as registration and verification. There are three parties that are involved in the registration process. They are known as RFID, backend server and reader. Both RFID tag and reader are registered with backend server. The server generates two numbers such as tracking sequence number and random number then

May – June 2020
ISSN: 0193-4120 Page No. 9461 - 9469

it computes a pseudo identity in the form of a tuple. Each tuple is made up of emergency keys and pseudo identities. Once registration is completed, the server sends credentials to the two parties. Those credentials are used later for mutual authentication process. Backend server provides required variables LAI_t, AID_T,EL,, N_x,V1. This information is bundled into $M_{A_1}(AID_T, N_x, Tr_{seq}(if\ required), S_{id}, EL, V_1)$ and sent to reader.

4.3 RFID Tag Side Operations

Generate: N_t

Compute:

$N_x = K_{ts} \oplus N_t$

$AID_T = h(ID_{T_j}||K_{ts}||N_t||Tr_{seq})$

|| operator for concatenation. AID_T is hashing functin of $ID_{T_j}||K_{ts}||N_t||Tr_{seq}$

$EL = LAI_t \oplus \mathrm{h}(K_{ts}||N_t)$

EL is Ex OR function of LAI_t and hashing function of $K_{ts}||N_t$

$V_1 = \mathrm{h}(AID_T||N_x||K_{ts}||R_i||S_{id}||EL)$

V_1 hashing function of $AID_T||N_x||K_{ts}||R_i||S_{id}||EL$

Or

$$pid_j \in PID, k_{em_j} \in K_{em}$$

$AID_T = pid_j, K_{ts} = k_{em_j}$

After receiving M_{A_1} by the reader from RFID, a random number is generated and N_y, K_{rs}, V_2, LAI_r is computed. Then the information is bundled into M_{A_2} (M_{A_2}: $\{N_y, R_i, V_2, LAI_r, M_{A_1}\}$) and sent to backend server so as to help in verification process.

4.4 RFID Reader Side Operations

Generate N_r

Derive $N_y = K_{rs} \oplus N_r$

N_y is Ex OR operation of $K_{rs} \oplus N_r$

Compute $V_2 = \mathrm{h}(M_{A_1}||N_r||K_{rs}||LAI_r)$

V_2 Hashing function of $M_{A_1}||N_r||K_{rs}||LAI_r$

After getting information from reader first it check with tracking number and simultaneously computes $AID_T K_{ts}$,N_x ,$R_i S_{id}$ and checks whether it is equal to V_1. If so, S computes N_t= $= K_{ts} \oplus N_x$, and then verifies AID_T and LAI_t withLAI_r .

If not, the session is terminated by the backend server. Once verification process is done successfully, a random number is generated and the tracking sequence number is updated. And then V_4 , V_3 are computed. This whole information is put into M_{A_3} and sends this M_{A_3} to reader. After receiving M_{A_3} computes $h(R_i||N_r||K_{rs})$ and verifieswhether it is equals to V_3. If it verifies so, R_i then sends M_{A_4} to Tj

4.5 Compute and Check Operations at Reader

$V_3^* = \mathrm{h}(R_i||N_r||K_{rs}) = V_3$

V_3^* is hashing function of $(R_i||N_r||K_{rs})$

4.6 Operations at Database Server

Check:?Tr_{seq}

Derive: $N_t = K_{ts} \oplus N_x, N_r = K_{rs} \oplus N_y$

Compute and verify:?V_2.? V_1.? AID_T and LAI_t $with$hLAI_r

Generate m:

Compute:$Tr_{seq_{new}} = m$

Tr=h($K_{ts}||ID_{T_j}||N_t) \oplus Tr_{seq_{new}}$

Tr is Ex OR operation of $Tr_{seq_{new}}$ and hashing function

$V_4 = \mathrm{h}(Tr||K_{ts}||ID_{T_j}||N_t)$

V_4 is hashing function of $Tr||K_{ts}||ID_{T_j}||N_t$

$V_3 = \mathrm{h}(R_i||N_r||K_{rs})$

$V_3 is$ hashing function of $R_i||N_r||K_{rs}$

After getting MA4, Tj computes and verifies whether it is equals to V_4

$$V_4^* = \mathrm{h}(Tr||K_{ts}||ID_{T_j}||N_t) = V_4$$

Compute and update:

$$Tr_{seq_{new}} = \mathrm{h}(K_{ts}||ID_{T_j}||N_t) \oplus Tr$$

$Tr_{seq_{new}}$ is Ex OR operation of Tr and hashing function.f

$K_{ts_{new}}$ =h($K_{ts}||ID_{T_j}||Tr_{seq_{new}}$)

$K_{ts_{new}}$ is hashing function of $K_{ts}||ID_{T_j}||Tr_{seq_{new}}$

$$Tr_{seq} = Tr_{seq_{new}}, K_{ts} = K_{ts_{new}}$$

May – June 2020
ISSN: 0193-4120 Page No. 9461 - 9469

Or

$K_{ts_{new}}$ =h($ID_{T_j}||k_{em_j}$) $\oplus x, K_{ts} = K_{ts_{new}}$

$K_{ts_{new}}$ *is* Ex OR operation of hashing function and x.

This authentication process ensures anonymity, provides secure end to end communications besides preserving privacy. The scheme exhibits many security features like mutual authentication process, security information availability, anonymity to improve security, usage of pseudo identity, usage of emergency key that is unlinkable, forward secrecy that does not allow adversaries to obtain details of old sessions, scalability to enable large scale usage of smart homes, secure localization and quick response. Thus the scheme prevents replay attacks and forgery attacks. It also prevents cloning attack. The usage of unlinkable pseudo identity and emergency key present attacks like Denial of Service (DoS).

5. EXPERIMENTAL RESULTS

This section presents details of experiments made. Different security attributes are studied on the proposed scheme. The security attributes and the observations made are presented in Table 2.

Scheme	**Mutual Authentication**	**Strong Anonymity**	**Availability**	**Forward security**	**Scalability**	**Secure localization**
[21]	*No*	*No*	*No*	*No*	*No*	*No*
[22]	*No*	*No*	*No*	*Yes*	*No*	*No*
[23]	*Yes*	*No*	*No*	*No*	*No*	*No*
[24]	*Yes*	*No*	*No*	*Yes*	*No*	*No*
Proposed	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*

Table 2: Performance evaluation of RFID based authentication schemes

As shown in Table 2, there is comparison made between the performance of proposed scheme and existing schemes in terms of various security attributes. It is found that all security features are supported by the proposed scheme. The scheme presented in [21] is not able to provide any features expected. Forward secrecy is supported by the scheme in [22]. In [23], mutual authentication is supported. Both mutual authentication and forward secrecy are supported by the scheme presented in [24]. The execution time of the schemes is also observed and presented in Table 3.

Scheme	**Execution Time (msec)**
[21]	0.65
[22]	0.45
[23]	0.78
[24]	0.65
Proposed	0.92

Table 3: Execution time comparison

As presented in Table 3, the time taken for execution is compared among the schemes. In the process, the proposed scheme showed 0.92 milliseconds that reflects that the scheme is taking more time. However, it showed better performance in terms of security features when compared with the other schemes. The scheme in [22] showed least execution time with 0.45 seconds. The time complexity of the proposed scheme is increased as it provides higher level security. This trade-off is understandable as far as security is to be given higher priority. The empirical study used face images for biometric authentication. The images are captured in different conditions and facial expressions with 256 grey level pixels with size 92x112.

May – June 2020
ISSN: 0193-4120 Page No. 9461 - 9469

Figure 5: An excerpt face images collected from [25]

Figure 5 shows an excerpt of the dataset collected. The face images are used for biometric authentication. As the tags and these faces are registered with backend server, the authentication process checks both of them. As many as 100 runs are used and the average results are provided in Table 3.

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
IMA with Proposed Scheme	9.90	12.02	18.34	10.12	10.23	12.12

Table 4: Average execution time comparison

Different image matching schemes are compared such as SURF, SIFT and IMA. The proposed scheme along with IMA is found to be better in security. However, its execution time is more when compared with other schemes.

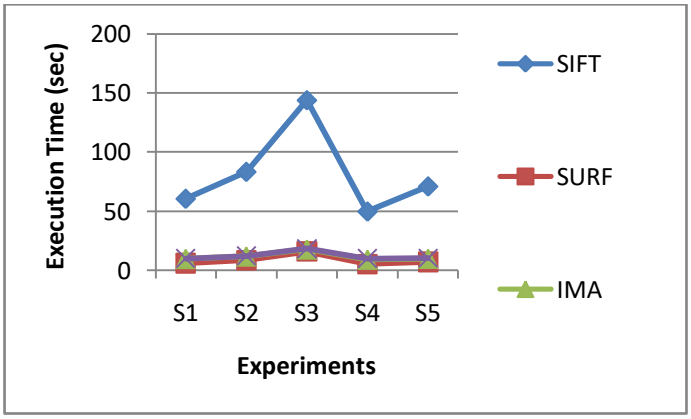

Figure 6: Performance evaluation with respect to image matching

As presented in Figure 6, different experiments are made and the execution time is observed for different image matching techniques. The execution time of the proposed scheme found less when compared with other schemes. Especially, it is better than that of SIFT technique. The IMA with the proposed scheme is found to have better performance over the SIFT approach.

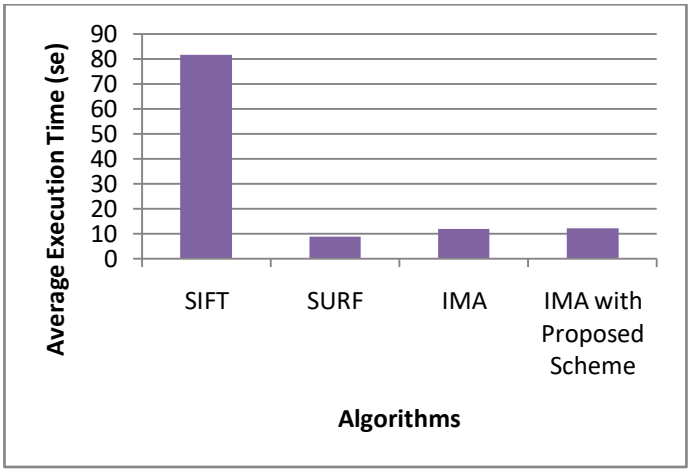

Figure 7: Performance comparison in terms of average execution time

May – June 2020
ISSN: 0193-4120 Page No. 9461 - 9469

As presented in Figure 7, the average execution time of the five experiments is provided. SURF showed least execution time SIFT showed highest execution time. IMA technique is much better than SIFT. However, the IMA with the proposed scheme has a little bit overhead but still it has comparable performance improvement over SIFT. From the results, it understood that the RFID and biometric based authentication provides higher level of security. It ensures secure communications among all the parties involved in the proposed system.

CONCLUSION

Of late, IoT technology integration paved way for different applications in the real world. The usage of IoT is increased as it is capable of combining digital and physical worlds. However, there are security and privacy issues as the IoT technology involves highly heterogeneous scenario. The security and privacy issues are investigated in this paper. A cloud based authentication system that uses RFID and biometric approaches is built for secure access to smart home. Besides it ensures secure end to end communications among the parties involved in the communication. Secure communications are made among RFID tag, its reader and database server. The proposed security scheme is implemented and evaluated. The results revealed that the proposed system shows better performance when compared with the state of the art. In future, the security framework is further enhanced to see that there is privacy preserving communication in smart home use case.

REFERENCES

1. 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.
2. Kemal Akkaya, Ismail Guvenc, Ramazan Aygun, Nezih Pala, Abdullah Kadri. (2015). IoT-based Occupancy Monitoring Techniques for Energy-Efficient Smart Buildings. *IEEE*, p1-6.
3. José L. Hernández-Ramos, M. Victoria Moreno, Jorge Bernal Bernabé, Dan García Carrillo and Antonio F. Skarmeta. (2014). SAFIR: Secure Access Framework for IoT-enabled Services on Smart Buildings. *Journal of Computer and System Sciences*, p1-24.
4. Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle. (2015). Privacy in the Internet of Things: Threats and Challenges. *ACM*, p1-14.
5. Antoni Martínez-Ballesté, Pablo A. Pérez-Martínez, and Agusti Solanas. (2013). The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City Is Possible. *IEEE*, p1-6.
6. Kuan Zhang, Jianbing Ni, Kan Yang, Xiaohui Liang, Ju Ren, and Xuemin (Sherman) Shen. (2017). Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE*, p1-8.
7. Alberto Huertas Celdrán, Félix J. García Clemente, Manuel Gil Pérez, and Gregorio Martínez Pérez. (2016). SeCoMan: A Semantic-Aware Policy Framework for Developing Privacy-Preserving and Context-Aware Smart Applications. *IEEE SYSTEMS JOURNAL*. 10 (3), p1-14.
8. Tuan Anh Nguyen and Marco Aiello. (2013). Energy intelligent buildings based on user activity: A survey. *Energy and Buildings*. 56, p244–257.
9. Pandarasamy Arjunan, Manaswi Saha, Haksoo Choi, Manoj Gulati, Amarjeet Singh, Pushpendra Singh, Mani B. Srivastava. (2015). SensorAct: A Decentralized and Scriptable Middleware for Smart Energy Buildings. *IEEE*, p1-10.
10. Sharad Mehrotra, Alfred Kobsa, Nalini Venkatasubramanian and Siva Raj Rajagopalan. (2016). TIPPERS: A Privacy Cognizant IoT Environment. *IEEE*, p1-6.
11. M. Kuzlu, M. Pipattanasomporn, and S. Rahman. (2015). Review of Communication Technologies for Smart Homes/Building Applications. *IEEE* , p1-6.
12. LIANG CHEN, SARANG THOMBRE, KIMMO JÄRVINEN, ELENA SIMONA LOHAN, ANETTE ALÉN-SAVIKKO, HELENA

May – June 2020
ISSN: 0193-4120 Page No. 9461 - 9469

LEPPÄKOSKI, M. ZAHIDUL H. BHUIYAN, SHAKILA BU-PASHA, GIORGIA NUNZIA FERRARA, SALOMON HONKALA JENN. (2017). Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey. *IEEE*. 5, p1-22.

13. Kaitai Liang,Joseph K. Liu, Man Ho Au and Rongxing Lu. (2016). Privacy-Preserving Personal Data Operation on Mobile Cloud - Chances and Challenges over Advanced Persistent Threat. *Elsevier*, p1-40.
14. Litun Patra and Udai Pratap Rao. (2016). Internet of Things – Architecture, Applications, Security and other Major Challenges. *IEEE*, p1-6.
15. Brian Cusack and Reza Khaleghparast . (2015). A privacy gap around the internet of things for open-source projects. *IEEE*, p1-8.
16. Aveek K. Das,Parth H. Pathak,Josiah Jee,Chen-Nee Chuah and Prasant Mohapatra. (2017). Non-Intrusive Multi-Modal Estimation of Building Occupancy. *ACM*, p1-14.
17. E. Ahvar, N. Daneshgar-Moghaddam, A. M. Ortiz, G. M. Lee, and N. Crespi. (2016). On Analyzing User Location Discovery Methods in Smart Homes: A Taxonomy and Survey. *Journal of Network and Computer Applications(Elsevier)*, p1-34.
18. Zhongliang Zhao, Stephane Kuendig, Jose Carrera, Blaise Carron, Torsten Braun, Jose Rolim. (2017). Indoor Location for Smart Environments with Wireless Sensor and Actuator Networks. *IEEE*, p1-8.
19. SRAVANI CHALLA, MOHAMMAD WAZID, ASHOK KUMAR DAS, NEERAJ KUMAR, ALAVALAPATI GOUTHAM REDDY, EUN-JUN YOON AND KEE-YOUNG YOO. (2017). Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications. *IEEE*, p1-16.
20. Magesh Kumar K, Vetripriya M, Brigetta A, Akila A, Keerthana D. (2016). Analysis on Internet of Things and Its Application. *IJSRSET*. 2 (2), p1-8.
21. Yang, J., Park, J., Lee, H., Ren, K. and Kim, K. (2005). Mutual authentication protocol forlow-cost RFID. Proceedings of the Workshop on RFID and Lightweight Cryptography, p17-24.
22. Tan, C. C., Sheng, B. And Li, Q. (2008). Secure and server-less RFID authentication and search protocols. IEEE Transactions on Wireless Communications, 7, p1400-1407.
23. Cai, S., Li, Y., Li, T. and Deng, R. (2009). Attacks and improvements to an RFID mutual authentication protocol. Proceedings of the 2nd ACM Conference on Wireless Netwrok Security, p51-58.
24. Cho, J. S., Jeong, Y. S. and Park, S. (2015). Consideration on the brute-force attack cost and retrieval cost: a hash-based radio-frequency identification (RFID) tag mutual authentication protocol, Computers and Mathematical Applications, 69, p58-65.
25. K. S. Niraja, Dr. Murugan : Security Risks in Internet of Things: A survey" International Conference on Computational Intelligence and Computing Research", 14th – 16th December, 2017
26. K. S. Niraja, Dr. Murugan :" security issues in the layered architecture of iot: a review" Recent Trends in Electronics Information &Communication Technology", 18th – 19th May, 2018.
27. Prof Andy Hopper FREng. (2002). Cambridge University Computer Laboratory. AT&T Laboratories Cambridge. Retrieved from http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html