International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-4, February 2019

RCAC: A Secure and Privacy Preserving RFID based Cloud-Assisted Access Control to IoT Integrated Smart Home

Gouse Baig Mohammad, U Ravi Babu

Abstract*: With the emergence of Internet of Things (IoT), smart and intelligent applications are being developed. One of the key enabling technologies of IoT is Radio Frequency Identification (RFID). RFID uniquely identifies all connected devices and things in an IoT use case like smart home which may be part of smart city use case in turn. Therefore IoT applications are implicitly made RFID critical. Thus ensuring security and privacy in RFID communications is indispensable for sustainable growth in such applications. With respect to smart home access control, there might be privacy attacks since RFID carries sensitive information of users. Cyber criminals may target to destroy critical digital infrastructure. RFID authentication is made large scale in IoT integrated applications. Therefore, it is essential to have cloud-assisted solution. With cloud integration, RFID authentication reaps benefits of cloud such as scalability, availability and fault tolerance at server side. Nevertheless, cloud is untrusted environment from user point of view and vulnerable to attacks. Therefore there is need for secure and privacy preserving RFID based authentication mechanism. Such system should be able to prevent both internal and external attacks. The mechanisms found in literature are using various schemes to implement security. However, consideration of probability of internal attacks solicits a new model for enhancing security in smart home use case. Towards this end, we proposed a secure and privacy preserving framework to safeguard interests of all stakeholders of the use case as far as security is concerned. The framework is known as RFID based Cloud-assisted Access Control (RCAC). It enables secure communications among parties involved in access control mechanism. It is lightweight, secure, privacy preserving and prevents external and internal attacks. Amazon EC2 is used as cloud platform to evaluate the framework. Experimental results are encouraging and RCAC shows performance improvement over the state of the art.

***Index Terms*: Radio Frequency Identification, Internet of Things, RFID based authentication, cloud assisted RFID authentication**

I. INTRODUCTION

Internet of Things (IoT) is the technology which is emerging. It is going to influence every field in the world. It has plenty of use cases like smart homes, smart cities, smart transportation, healthcare and so on. The transition in computing and the technologies with innovations from time to time led to the IoT technology. It enables masses to be creative and provides plethora of opportunities in an unprecedented fashion. However, it also brings its challenges and issues. Especially security is one of the major issues that need to be addressed to have sustainable growth of applications that need cloud and IoT eco-system [15]. IoT has many enabling technologies like RFID, communication protocols, sensor networks, Near Field Communication (NFC), etc. [16]. IoT architecture has different layers like perception layer, transportation layer, business layer, processing layer, and application layer. IoT middleware software enables rapid application development leading to smart applications [17]. With IoT, smart applications realize benefits like any time connection, any place connection and anything connection [18]. Smart home is one of the RFID critical IoT enabled applications where security is to be given paramount importance. Smart home is essentially part of a smart city application in general. Therefore, the IoT integrated critical digital infrastructure needs to be protected from cyber attacks. Different cloud based authentication schemes explored in [6], [9], [10] and [12] came into existence. There are some issues to be addressed. First, there might be internal attacks at cloud server to steal RFID tag information. Or it may be done by using a compromised RFID reader. Second, privacy attacks may occur on RFID tags. Third, any external attacks may be launched by adversaries as RFID is vulnerable in the ether. From the literature it is understood that it is still desired to have a framework for solving all the problems related to security and privacy in smart IoT applications. Our contributions of the paper are as follows.

1. We proposed a framework to have secure and privacy preserving RFID based cloud assisted authentication. The framework is named as RFID based Cloud-assisted Access Control (RCAC) which is light weight and prevents privacy, internal and external attacks.
2. Amazon EC2 cloud platform based implementation is made with three important components encapsulating issuer, tag reader and server. Server and issuer components run in cloud while tag reader runs in the local host to demonstrate proof of the concept.
3. Detailed security analysis is made and the insights are provided.

The remainder of the paper is structured as follows. Section 2 provides review of literature on secure authentication protocols and cloud based RFID authentication protocols existed in the literature. Section 3 presents IoT integrated smart home use case, its enabling technologies, communication protocols and RFID security challenges.

Manuscript published on 28 February 2019.
***Correspondence Author(s)**

Gouse Baig Mohammad, Research Scholar, Acharya Nagarjuna University, Asst. Prof., Dept. of IT, Muffakham College of Engineering & Technology, Hyderabad, India.
Dr. U Ravi Babu, Principal, DRK College of Engineering & Technology, Hyderabad, India.

Section 4 presents the proposed framework and its mechanisms for preventing internal and external threats. Section 5 provides experimental setup based on Amazon EC2 platform. Section 6 presents experimental results.
Section 7 evaluates experimental results. Section 8 concludes the paper and provides directions for future scope of the research.

II. RELATED WORK

This section provides review of literature on authentication and access control mechanisms in RFID critical systems. Alam et al. [1] investigated the state of the art of smart homes. Smart home is the application ubiquitous computing. Smart home may have features related to comfort, healthcare and security. Smart homes provide next generation environments in cities. However, they need to have secure access control mechanisms [8], [13]. The following sub sections review on authentication schemes for IoT applications and cloud based RFID authentication schemes.

A. Authentication Schemes for IoT Applications

Hernández et al. [2] proposed location-aware approach in access control to smart buildings. They encapsulated access control engines into smart objects. Secure localization and access control mechanisms are explored. Kumar et al. [3] on the other hand defined a framework which is anonymous and provides secure communications among connected devices in smart homes. Bugeja et al. [4] explored security challenges in smart home applications. The challenges are related to resource constraints, mobility, heterogeneous protocols, dynamic characteristics and longevity expectations. They identified different levels of security such as device level, communication level and service level. Smart city applications also have such security issues [7].

Recent developments in home Machine to Machine (M2M) networks include emergence of M2M devices, M2M ad hoc networks, Internet of Things (IoT) and RFID [5]. Samad et al. [11] proposed an RFID based authentication as part of animal data recording and tracking system. Mahalle et al. [14] proposed a new authentication model for IoT based use cases. It is known as Identity Authentication and Capability based Access Control (IACAC). Liu et al. [19] reviewed access control and authentication mechanisms in IoT integrated applications. Jan et al. [20] proposed a robust authentication scheme which is light weight and provides mutual authentication. Without proper authentication mechanisms, IoT architectures are vulnerable to attacks.

Challa et al. [21] proposed signature based scheme for secure communications in IoT applications. The secure key establishment here ensures security against eavesdropping, Denial of Service (DoS) and a host of other attacks. Turkanovi et al. [22] defined novel user authentication and key agreement schemes in IoT environments. Rizzardi et al. [23] on the other hand proposed authentication mechanisms in publish/subscribe model for Internet of Things applications. The notion of semantic service objects including security is introduced for IoT applications in [24] while RFID based tracking; locating and controlling mechanisms are explored in [25].

B. Cloud Based Authentication Schemes

Cloud computing resources enable smart applications to gain benefits of cloud. Gope et al. [6] proposed a secure and privacy preserving RFID based secure authentication scheme with secure localization. This scheme is somewhat close to the work of this paper as far as cloud is used in the authentication mechanism. Since smart home is an IoT integrated application, cloud resource utilization is essential as studied in [9]. IoT workflow applications are even suitable for the environment where fog computing is used [10]. Xie et al. [12] implemented a cloud based authentication based on RFID. They contributed to a server less RFID architecture where communication takes place between RFID tag, reader and cloud take place.

As found in the literature, it is understood that RFID is widely used for uniquely identifying objects, tracking them and even communicating with other parties to realize IoT use cases. Therefore it is crucial to protect RFID based communications. The existing RFID based authentication mechanisms for smart applications are to be improved further in terms of preventing both internal and external attacks. When tag reader is compromised or when server side keys are stolen security will be lost for smart home. This problem is addressed in this paper.

III. SMART HOME, ENABLING TECHNOLOGIES AND PROBLEM CONTEXT

This section provides fault diagnosis model for security. The model here computes the level of security provided by a node and makes use of communication fault probability function S(q). Fault probability reflects the node’s rate of interactivity and energy at different intervals. Assuming a node has many neighbor nodes. The probability interact ion is computed as follows.

As explored in [1], [8] and [13], there are plenty of IoT integrated applications. Smart home is no exception. This section provides different aspects of smart home, its enabling technologies connected to IoT, communication protocols and so on.

A. Typical Smart Home Use Case

Smart home is an IoT integrated application. In this kind of application the home appliances are made smart and integrated with mobile and Internet communications. It can be used to have smart control to the equipment of home and also electronically access the accessories to control them. Different stakeholders may coexist with IoT use case such as surveillance firm, healthcare providers, entertainment providers, and others. Different sensors are involved to sense present situation and send messages to server and users of smart home.

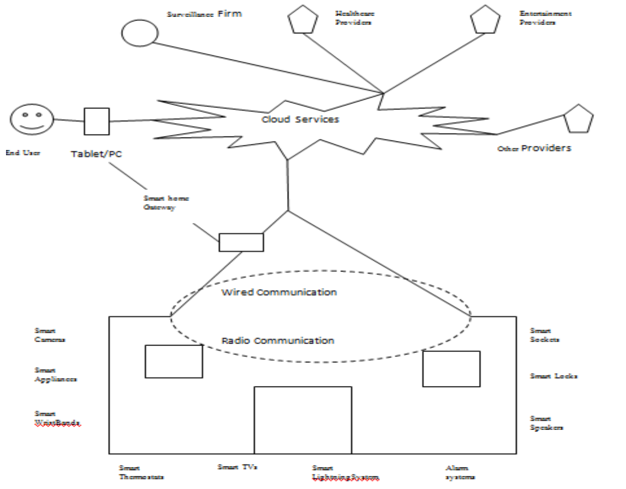


Figure 1: Smart home environment

As shown in Figure 1, the smart home is equipped with smart objects, wired and wireless communications and security mechanisms. However, there are many security challenges as exploredin [15]. Access control is one of the challenging issues in smart home. Access control needs device authentication and object authentication as well. Different communication protocols, telecommunications, Internet, mobile devices and other smart applications are integrated in general. There are different stakeholders who need to be satisfied with the proposed security. This smart home use sae is considered in this paper for making an empirical study on RFID based secure and privacy preserving authentication.

B. Stakeholders of Smart Home

RFID critical applications like smart home is integrated with many other stakeholders. It is illustrated in Figure 2. It does mean that smart home is not realized unless there are many parities involved. Smart home application is linked to other service providers or stakeholders.

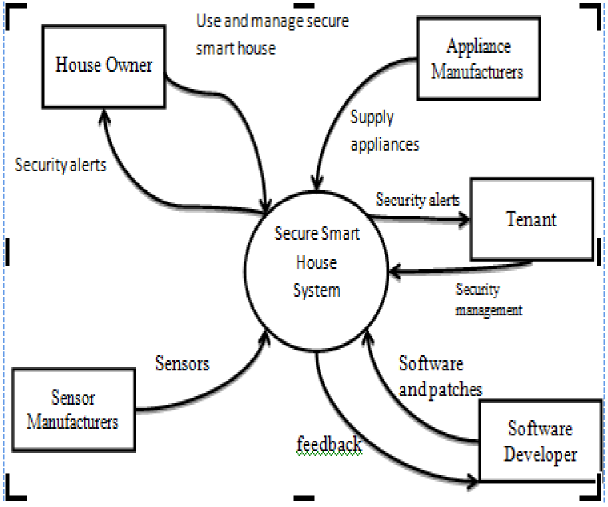


Figure 2: Stakeholders in the context of a secure smart home system

As shown in Figure 2, smart home is linked to various parties like appliance manufactureres, softwware development companies, sensor manufactuers, platform providers and even police to have access to security provided by police as and when needed. Security implemntations are esential for having timely security alerts. As far as access control is considered, it is essential to have highly secure commmunications. In the process security alerts may be sent to house owners, tenants and even police associated with the use case.

C. RFID and Internet Of Things

Internet of Things technology enables connectivity between digital and physical objects while RFID enables identity and communication among connected devices. When millions of connected devices exist, IoT adds more value as per Metcalfe's law which states that the number of nodes bestows value proportionately. Objects and things connected are context-aware and they can interact with other devices forming M2M. Customized, user-friendly and smart applications are possible with IoT integration. For instance, in healthcare, real time healthcare monitoring is possible with IoT and its associated body wearable sensors. Since IoT creates higher and unprecedented value to its stakeholders, different smart applications co-exist in the computing arena forming critical digital infrastructure which may be targeted to external and internal attacks. This paper is therefore related to secure communications in smart applications.

RFID plays pivotal role in realization of IoT applications. IoT needs specific requirements such as technology for device and thing identification and tracking, wireless sensor network for smart sensing, wireless infrastructure with global standards, robust middleware, nano technology to reduce size of devices and sensors so as to embed in other things, energy efficiency, securable, locatable, controllable, readable, recognizable objects. In order to realize IoT, RFID is very pervasive and needed by every smart application in the world. However, RFID technology is vulnerable to many security threats. Security and privacy issues are to be addressed and further standards are needed to make it robust and resilient against adverse attacks. RFID is used to identify objects, therefore, its data needs to be secured and non disclosure of sensitive data needs to be taken care of. RFID tags may be subjected to two kinds of attacks such as internal and external. The pervasiveness of RFID is more in presence of IPv6 protocol.

D. Communication Protocols

IoT integrated smart home relies on different communication protocols. This is essential as there needs to be communications among different parties. There is need for short and wide range protocols to support data transport among devices and connected things. Most widely used short range wireless communication technologies are Wi-Fi, IEEE 802.11p, WiMAX, Bluetooth and ZigBee. These short range protocols are used in applications like vehicular networks, healthcare and smart metering. There are wide range technologies needed by many IoT integrated applications. They include Global Packet Radio Service (GPRS), Global System for Mobile Communication (GSM) and Long Term Evolution (LTE). These technologies are used in infotainment, smart grid, mobile e-healthcare and Vehicle to Infrastructure (V2I) applications. There are other projects like Cellular IoT (C-IoT), SIGFOX, LoRaWAN,

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

LoRaAlliance and Third Generation Partnership Project (3GPP) going on to have more possibilities in the area of IoT applications.

E. Security Challenges of RFID Critical Applications

Along with many benefits, RFID brings many challenges. RFID data quality and utility is one of the challenges. To overcome this, enterprises need to consider it in their data management system. When organizations are not able to exploit RFID data, this technology is of less use in certain applications like Supply Chain Management (SCM). When RFID data flows across an application, it is exposed to different attacks. Typically, security threats to RFID are in the air. Eavesdropping may occur when communication between tag reader and RFID tag is listened by adversaries. Large read range of RFID also paved way for possible attacks. Rogue readers may exploit sensitive information. Distance authentication mechanism needs to be used to alleviate this. Data shielding needs to be made from avoiding intercepting from rogue readers. Reader authentication is another possible solution. Attackers may also use blocker tags in order to launch Denial of Service (DoS) attack. There are some security attacks with unauthorized RFID tags. Fake tags may be used to have replay attacks. Transfer of ownership issue is also there with RFID besides multiple authorizations. The tags can have either static or dynamic data or both at a time. RFID tags may carry sensitive information. Therefore it is vulnerable to privacy disclosure attacks. If RFID tags data is manipulated by adversaries, it will affect two kinds of queries made on RFID data management system. The queries are known as object monitoring and object tracking. As RFID technology is still evolving, there might be many not yet known vulnerabilities or threats. Tag cloning is another security issue of RFID technology. Location privacy is to be addressed as it reveals sensitive information to adversaries.

IV. PROPOSED SYSTEM

This section provides methodology for cloud-assisted RFID authentication for smart home access control. Cloud-assisted authentication is proposed without the need for overhead of Certificate Authority (CA) or Trusted Third Party (TTP). Our authentication framework presents secure communication between RFID tag reader and cloud server. The framework also defeats insider attacks. It employs threshold cryptography for achieving this. The framework also reduces overhead in the server and ensures that the location privacy of the RFID reader is not lost. Before diving into the technical details it is good to understand the problem clearly.

A. Problem Statement

IoT applications need diversified devices and protocols from various vendors. The devices obviously differ in standards, size, energy usage, storage, data rate and computations. By embedding sensors and actuators in such devices or things, seamless integration is achieved. The miniature sensors are identified with RFID where RFID tags contain identify information. In this environment privacy, trust and security provision is very challenging. IoT use cases are unduly complex and they need to face security challenges. In the domain of IoT security research is still at its inception and much more needs to be done. There is chance of any device to act as malicious. The sensors and smart phones used in the network are susceptible to attacks. When sensor data is intruded and manipulated, it causes havoc to IoT integrated applications like smart home and healthcare to mention few. When IoT applications are integrated with cloud computing and even fog computing, there are more changes of using wide open standards and the attack possibility is more. Many existing cloud assistedsmart applications have provided secure communications. However, there are chances of compromising a reader or indulging into insider attacks at server side to steal tag information. IN such cases smart home security is lost and unauthorized users may be able to access smart home. Thus it is challenging to have a more resilient framework for preventing outsider and insider attacks pertaining to either security or privacy. The following sub sections provide the details of the proposed framework and security mechanisms.

B. The Framework

This section provides the proposed framework and its details. The framework has three important components. They are known as issuer who provides security keys, tag reader which reads tag information and server which performs authentication. Threshold encryption is used in the security mechanisms based on EIGamal encryption. Each component is given a unique decryption share provided by issuer to all parties involved.

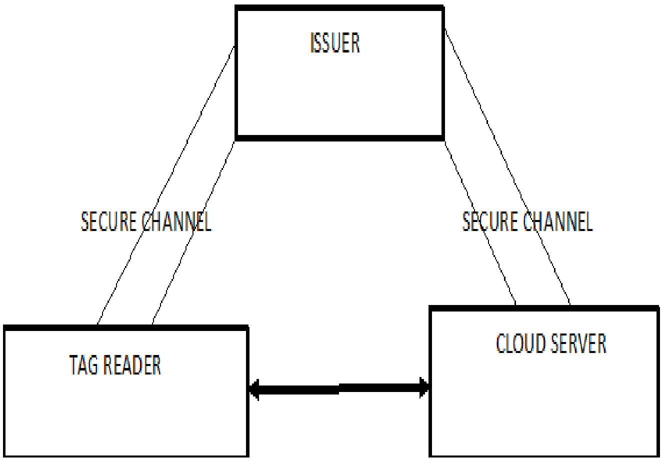


Figure 3: Overview of RCAC framework

As illustrated in Figure 3, the cloud server plays pivotal role in RFID based authentication proposed. The trustworthiness is not assumed in the framework. It is unlike other schemes existing in the literature. When private keys are stolen at server side, or if the private keys are disclosed for any reason or corrupted RFID tags also, the proposed framework still works fine.

It does mean that it can withstand internal attacks and external attacks. It also ensures privacy of data involved in communications. The proposed scheme does not allow internal attacks.

Table 1: Provides notations used in the proposed framework

Notation	Description
$f(x)$	Secret curve
a_0	The private key
h	Public key.
(x^S, y^S)	Server own key share
(x^i, y^i)	Unique secret share of ith tag of object
I	Object tag
$m = r^S \| r^i$	ElGamal encryption of message
Zq	Primary numbers set
C	Encrypted message pair
σ	Decryption share
σ_s	Decryption share of the server
σ_i	Decryption share of tag i
Q	Prime number
M	Message
R	Random prime number
R	Random parameter set with 0,1
L	Security parameter
S	Server
G	Generator

The cloud server has many pre-computed encryption keys to have secure communications besides reducing overhead. The security keys, prime numbers, unique secret shares, secret polynomials are generated by the issuer. Secure communication channel exists between issuer and other parties in the framework. The tag reader is responsible to take RFID tags and help in tag authentication to be carried out in the proposed framework. Unique RFID tag is associated with each entity in the smart home case study. Each RFID tag contains its security share and that of server given publicly. More details of the framework are provided in Section 4.3.

C. Functionality of RCAC Framework

This section describes the actual protocol or the scheme used in the proposed framework. It provides communication dynamics among cloud server, tag reader and issuer. Table 1 shows the details of the notations used in this scheme.

1. Each server in the proposed framework maintains its share key denoted as(x^S, y^S). It is required to be maintained by server for both encryption and decryption purposes.
2. Every entity involved in smart home use case is given a single RFID tag. It is denoted by *i*. It is used to compute share key for the entity as denoted by(x^i, y^i).
3. Once share keys are generated for each server and each entity, the information of entities is encrypted and saved in cloud server.
4. With respect to encryption and decryption the required keys are obtained. First, entity chooses a random number denoted as$r^i \in_R \{0,1\}^l$. Afterwards, it that number is sent to server and 1 is considered as security parameter.
5. The cloud server chooses a random number denoted as$R^s \in_R \{0,1\}^l$. Then it computes something known as ElGamal encryption of a message denoted as m=$r^S \| r^i$.
6. In order to encrypt m (the message) a random prime number denoted as r ∈ Zq is considered. This number is used to compute $C = (h^r m, g^r)$ which denotes an encryption pair. It is also required to calculate decryption share denoted as$\sigma = g^r y^S$. Afterwards the server needs to send encryption pair and decryption share to ith tag of the entity.
7. Once the message σ, C are received from server the entity computes decryption share pertaining to server which is denoted as$\sigma_s = \sigma^{\frac{x^i}{x^i - x^S}}$.
8. Afterwards, decryption share denoted as $\sigma_i = g^{ryi\frac{x^S}{x^S - x^i}}$is computed.
9. Then the original message is recovered denoted as$r^{\sim S} \| r^{\sim i} = \frac{h^r m}{\sigma_s \sigma_i}$.
10. Comparison is made between r^i and $r^{\sim i}$ and $r^{\sim S}$ is assigned to$\hat{r}$. And it is sent to server where verification between $\hat{r}$ and $r^S$are made.
11. If the r^i is not equal to $r^{\sim i}$ one random value is chosen and assigned to $\hat{r}$ and then set to server where server verifies $\hat{r}$withoriginalr^S.

V. EXPERIMENTAL SETUP

Amazon EC2 cloud is used for empirical study. The proposed framework RCAC is realized by implementing three components. The components are implemented to encapsulate the three important parts of the RCAC framework. They are known as issuer, server and tag reader. EC2 cloud is used to execute issuer and server components. In other words, they run in a remote system and provide required functionalities required by the system for RFID based authentication. The tag reader component is executed in the local host. The communication mechanisms among the components as described in Section 4.

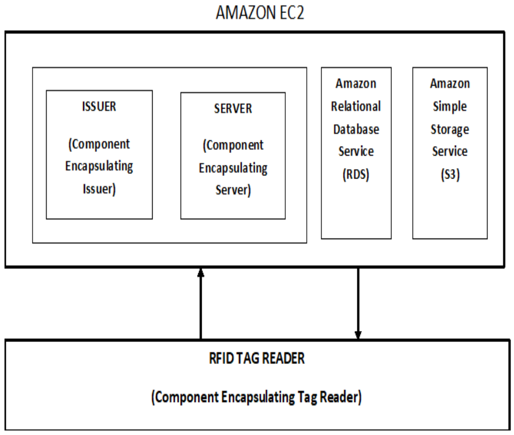

AMAZON EC2
ISSUER
(Component Encapsulating Issuer)
SERVER
(Component Encapsulating Server)
Amazon Relational Database Service (RDS)
Amazon Simple Storage Service (S3)
RFID TAG READER
(Component Encapsulating Tag Reader)

Figure 4: Experimental setup with Amazon EC2 cloud platform

As shown in Figure 4, there will be interaction among the components. The proposed framework and its underlying security mechanisms are tested using these components. The experimental results are observed to make conclusions.

The proposed framework is thus realized to have secure and privacy preserving RFID based cloud assisted authentication and access control to smart home application.

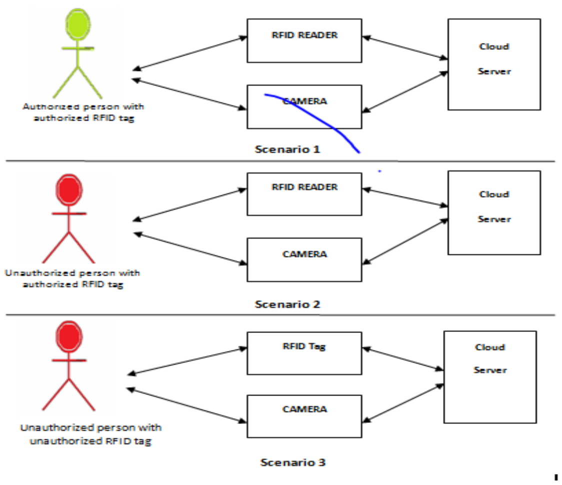

RFID READER
CAMERA
Cloud
Server
Authorized person with authorized RFID tag
Scenario 1
RFID READER
CAMERA
Cloud
Server
Unauthorized person with authorized RFID tag
Scenario 2
RFID Tag
CAMERA
Cloud
Server
Unauthorized person with unauthorized RFID tag
Scenario 3

Figure 5:Secure access control requirements of smart home use case

As presented in Figure 5, the smart home application has three scenarios pertaining to secure access control. RFID tags are issues to residents of smart home. Those who do have RFID tags issued by competent authority can access smart home. However, it has different possibilities or scenarios where security may be compromised if an efficient authentication mechanism is not in place. The solution provided in this paper focused on RFID based authentication. In our previous work, we implemented a base line approach for secure access control in smart home applications. However, this paper has addressed issues like internal threats, external threats and privacy attacks.

VI. EXPERIMENTAL RESULTS

The results of experiments are provided in this section. A synthetic dataset containing different sets of tags and RFID tag readers is used in the empirical study. There are 12 sets of experiments made. Each set of experiments has different number of tags and tag readers. The experiments are made using Amazon EC2 environment provided in the Section 5. The results are compared with state of the art authentication schemes like RSLA, AnonPri, RSGA and SPA as explored in [25].

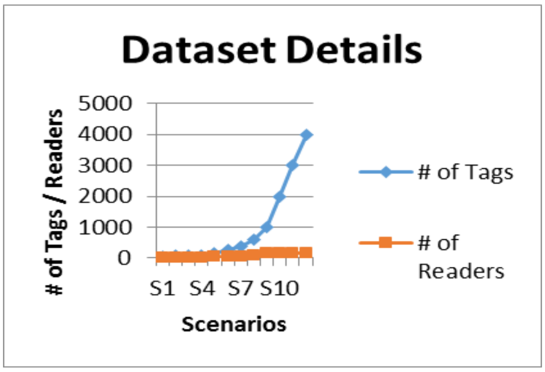


Figure 6: Dataset used to help experiments

As presented in Figure 6, the seven sets of experiments are provided in horizontal axis while the vertical axis provided number of tags or number of readers. For instance, there are 65 tags used in the first set of experiments while 10 tag readers are used. In the last set of experiments, 150 readers and 4000 RFID tags are used.

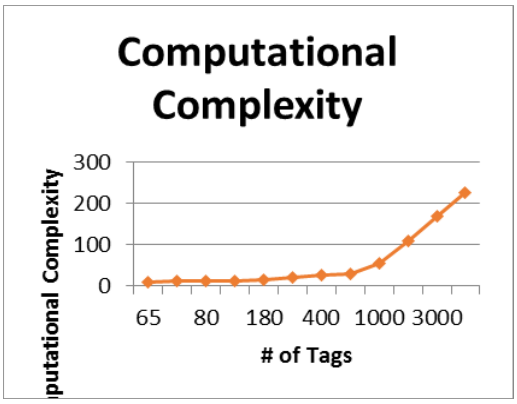


Figure 7: Computational complexity

As presented in Figure 7, the computational complexity of the proposed framework is provided. The number of tags used for the 12 sets of experiments is presented in horizontal axis while vertical axis shows the computational complexity. The results revealed that the computationally complexity is increased linearly when number of tags is increased in the empirical study.

Table 2: Performance in terms of authentication speed

No of tags	Authentication Speed (seconds)			
	RSLA	AnonPri	RSGA	RCAC
256	20	5	18	5
512	24	4	20	5
1024	28	20	24	5
2048	0	30	26	5
4096	32	40	23	5
8192	36	120	25	5

As shown in Table 2, the authentication time taken by the proposed and existing algorithms is presented against given number of tags. As shown in Figure 8, experiments are made with different number of tags as presented in horizontal axis. The authentication time taken is presented in vertical axis. The number of tags has its influence in the authentication time taken. However, the proposed scheme showed better performance over the state of the art approaches such as RSLA, AnonPri and RSGA.

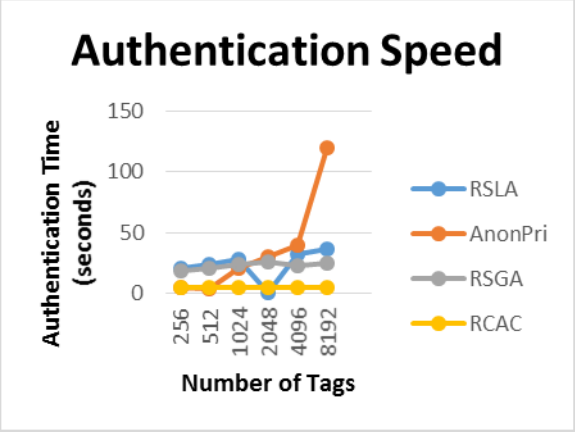
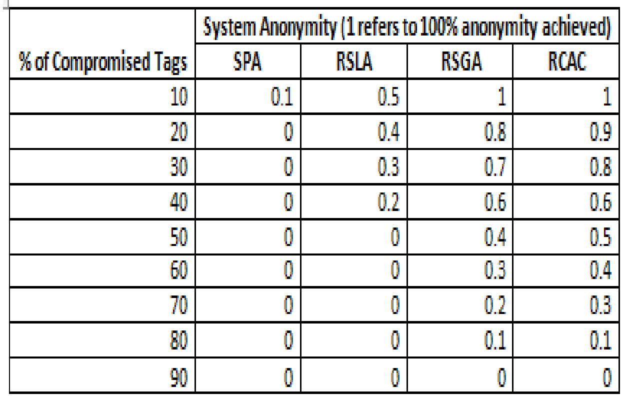


Figure 8:Number of tags vs. authentication time

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Table 3: Performance in terms of system anonymity



% of Compromised Tags	System Anonymity (1 refers to 100% anonymity achieved)			
	SPA	RSLA	RSGA	RCAC
10	0.1	0.5	1	1
20	0	0.4	0.8	0.9
30	0	0.3	0.7	0.8
40	0	0.2	0.6	0.6
50	0	0	0.4	0.5
60	0	0	0.3	0.4
70	0	0	0.2	0.3
80	0	0	0.1	0.1
90	0	0	0	0

As shown in Table 3, the system anonymity percentage exhibited by the proposed and existing algorithms is presented against given number of tags.

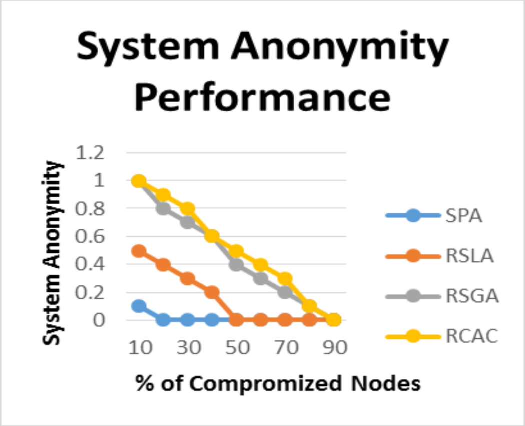


Figure 9: Shows percentage of compromised nodes vs. system anonymity

As presented in Figure 9, the percentage of compromised nodes is shown in horizontal axis and vertical axis shows system anonymity percentage which is measured between 0.1 and 1.0. The system anonymity is decreased with number of compromised nodes. However, the performance of the proposed system is better than the state of the art.

VII. EVALUATION

This section provides evaluation of the proposed work. The authentication scheme works even the private keys at server side or at the tag reader are compromised. When server is compromised, two attacks may be possible. Adversary may pretend as semi-honest party complying rules of protocol to obtain details of the tag. As the tag has sensitive data, it leads privacy problem. According to the proposed framework it is not possible to obtain tag information by the adversary as it is dynamic in nature. However, adversary may get a numeric value which is not the true identity of the tag. The second means of attack is made using server's compromised credentials to decrypt secret shares. It also fails as the random bits are sent by tag reader. This is related to security. When cloud server machine is compromised the secret keys are known to adversary. However, adversary will not be able to find actual tag data with the help of observations on communications. Thus the framework achieves both backward and forward secrecy. Next important feature is unlinkability. It refers to the fact that adversary cannot find tag details with the help of observed communications. In other words, the generated messages according to protocol will not disclose any information related to identity. Random numbers are used in step 1 and step 3. For this reason, there is no chance of revealing tag identity. Even the tag information obtained by adversaries cannot be mapped to any specific tag as the information is in encrypted form. With respect to complexity or overhead of the proposed framework, it involves less number of computations. The computations include a single multiplication operation, 3 inversions and 3 exponentiations. Nevertheless, it is possible to carry out inversions offline at tag reader. At server side the computations include a single multiplication operation and 3 exponentiations. Moreover, the server side operations like encryptions and partial decryption can be done offline. The overall complexity of the system will be intact even when new tad new tag. When a new user joins and gets new share, the computations remain same without causing additional burden to server. However, overall linear complexity is there.

VIII. CONCLUSION AND FUTURE WORK

A framework by name RFID based Cloud-assisted Access Control (RCAC) is proposed. It is meant for providing secure access control to a smart home. In the view of need for round the clock service availability, the authentication mechanism is cloud based. Thus it is made available, scalable besides enabling on-demand access control. The framework provides secure interactions among different parties like issuer, RFID reader and server. Security keys are provided to all by issuer. A secure channel is used for key sharing. Server and RFID reader have mutual authentication mechanisms. The framework has security mechanisms developed in such a way that it will not fail even if reader is compromised or private keys are stolen at server by insider attacks. Three software components are built to encapsulate the functionalities of the three parties aforementioned. Amazon EC2 is managed cloud platform used for empirical study. The server and issuer run in cloud while tag reader is executed in the local host. The framework is made light weight besides able to prevent insider attacks. Experimental results revealed that the RCAC is able to achieve its design goals with respect to security and privacy preserving access control to smart home. Moreover, it is found to be better than state of the art schemes found in literature. Further investigation into problems like tag tampering and ownership transferring is left for future work

REFERENCES

1. Muhammad RaisulAlam, M. B. I. Reaz and M. A. Mohd Ali.(2012). A Review of Smart Homes – Past, Present, and Future. *IEEE Transactions on Systems Man and Cybernetics Part C*, p1-16.
2. Pardeep Kumar, AnBraeken, Andrei Gurtov, JariIinatti and Phuong Hoai Ha. (2017). Anonymous Secure Framework in Connected Smart Home Environments. *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*.12 (4), p968-979.
3. José L. Hernández · M. Victoria Moreno · Antonio J. Jara · Antonio F. Skarmeta. (2014). A soft computing based location-aware access control for smart buildings. *3*, p1-16.

4. Joseph Bugeja, Andreas Jacobsson and Paul Davidsson. (2016). On Privacy and Security Challenges in Smart Connected Homes . *European Intelligence and Security Informatics Conference*, p172-175.
5. Min Chen, Jiafu Wan, Sergio Gonz´alez, Xiaofei Liao and Victor C.M. Leung. (2014). A Survey of Recent Developments in Home M2M Networks. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*.16 (1), p98-114.
6. ProsantaGope, Ruhul Amin, S.K. Hafizul Islam, Neeraj Kumar, Vinod Kumar Bhalla .(2017). Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. *ELSEVIER*, p1-10.
7. Kuan Zhang, Jianbing Ni, Kan Yang, Xiaohui Liang, JuRen, and Xuemin (Sherman) Shen. (2017). Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE*, p122-129.
8. JORDI MONGAY BATALLA, ATHANASIOS VASILAKOS AND MARIUSZ GAJEWSKI. (2017). Secure Smart Homes: Opportunities and Challenges. *ACM Computing Surveys*.50 (5), p1-32.
9. Christos Stergioua , Kostas E. Psannis, Byung-GyuKimb, Brij Gupta. (2018). Secure integration of IoT and Cloud Computing. *ELSEVIER*.78, P964–975.
10. Mung Chiang and Tao Zhang. (2016). Fog and IoT: An Overview of Research Opportunities. *IEEE INTERNET OF THINGS JOURNAL*.3 (6), P854-864.
11. Abdul Samada, PrashantMurdeshwar, ZohaibHameed. (2010). High-credibility RFID-based animal data recording system suitable for small-holding rural dairy farmers. *ELSEVIER*.73, P213–218.
12. Wei Xie1 , Lei Xie2 , Chen Zhang1 , Quan Zhang1 and Chaojing Tang. (2013). Cloud-based RFID Authentication . *IEEE International Conference on RFID*, p168-175.
13. Terence. K. L. Huia, R. Simon Sherratta , Daniel D´ıazS´anchez. (2015). Major Requirements for Building Smart Homes in Smart Cities based on Internet of Things Technologies, p1-20.
14. Parikshit N. Mahalle, BayuAnggorojati, Neeli R. Prasad and Ramjee Prasad. (2013). Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things. *Journal of Cyber Security and Mobility*. 1, p 309–348.
15. Dieter Uckelmann, Mark Harrison and Florian Michahelles. (2011). Architecting the Internet of Things, p1-378.
16. Dr. V. Bhuvaneswari and Dr. R Porkodi. (2014). The Internet of Things (IoT) Applications and Communication Enabling Technology Standards: An Overview. *International Conference on Intelligent Computing Applications*, p324-329.
17. PallaviSethi and Smruti R. Sarangi. (2017). Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*, p1-26.
18. Benjamin Khoo. (2014). RFID - from Tracking to the Internet of Things: A Review of Developments. *IEEE*, p1-9.
19. Jing Liu and Yang Xiao and C. L. Philip Chen . (2012). Authentication and Access Control in the Internet of Things . *32nd International Conference on Distributed Computing Systems Workshops*, p588-592.
20. Mian Ahmad Jan, Priyadarsi Nanda, Xiangjian He, Zhiyuan Tan and Ren Ping Liu. (2014). A Robust Authentication Scheme for Observing Resources in the Internet of Things Environment. *IEEE*, p1-8.
21. SRAVANI CHALLA1 , MOHAMMAD WAZID1 , ASHOK KUMAR DAS, NEERAJ KUMAR, ALAVALAPATI GOUTHAM REDDY3 , EUN-JUN YOON4 , AND KEE-YOUNG YOO. (2017). Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications. *IEEE. Translations and content mining are permitted for academic research onl*. 5, p3028-3043.
22. MuhamedTurkanovic, BoštjanBrumen, Marko Hölbl. (2014). A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. *ELSEVIER*.20, p96–112.
23. Alessandra Rizzardi a , Sabrina Sicaria,n , Daniele Miorandi b , Alberto Coen-Porisini . (2016). AUPS: An Open Source AUthenticated Publish/Subscribe system for the Internet of Things. *ELSEVIER*.62, p29–41.
24. Son N. Han, Noel Crespi. (2017). Semantic service provisioning for smart objects: Integrating IoT applications into the web. *ELSEVIER*.76, p180–197.
25. Yudai Komori, Kazuya Sakai, Satoshi Fukumoto, Fast and Secure Tag Authentication in Large-Scale RFID Systems Using Skip Graphs, Computer Communications (2017), doi: 10.1016/j.comcom.2017.11.008.