ISSN No. 0976-5697

Volume 8, No. 4, May 2017 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Review on Radio Frequency Identification Techniques and their usage for securing IOT

Er. Simranpreet Kaur
M.Tech Scholar, Department of Computer Science and Engineering, Guru Nanak Dev University Regional Campus, Jalandhar
Simranghotra22@gmail.com

Er. Varinder Kaur Attri
Assistant Professor, Department of Computer Science and Engineering, Guru Nanak Dev University, Regional Campus, Jalandhar
Varinder2002@yahoo.com

***Abstract*—This paper represents that development of the internet has lead the way to the exposure of internet of things (IoT). Radio-frequency identification is one of the familiar technologies used for the deployment of IoT. Currently, RFID based systems are the broadly dispersed applications for the purposes of tagging and tracking in the IoT formation. The RFID systems undergo through many attacks and security hazards. The overall objective of this paper is to discuss the various encryption techniques to eliminate the vulnerabilities that determine a set of security features likes mutual authentication, anonymity and confidentiality.**

***Keywords*-IOT; RFID; Authentication protocol; ECC; ECDH.**

I. INTRODUCTION

The Internet of Things (IOT) paradigm is based on smart and self constructing nodes interconnected in a active and global network framework. Iot represents the most disturbing technologies, enabling universal and omnipresent computing scenarios. IOT is commonly characterized by persistent world small things, universally distributed, with finite storage capacity and processing capacity, which consist of interests regarding reliability, performance, security and privacy. IOT is a platform in which unique identifiers are provided for things, people and animals that are able to transfer data over a network without requiring any man-machines or man-to-computer machines interaction. IOT has developed from the convergence of, micro-electromechanical systems, wireless technologies and the Internet. The Internet of Things, frequently called Internet of Everything is the network of objects integrated with software, sensors, electronics and connectivity to allow objects to exchange data with the constructor, operator and/or other attached devices. The objects in this criterion are allowed to be observed and controlled remotely over existing network infrastructure, providing convenience for direct connection between the real world and computer-machines, which is resulting in enhanced accuracy, efficiency and commercial benefit. Objects are uniquely identifiable through their integrated computing system but are capable to interoperate within the current Internet infrastructure.

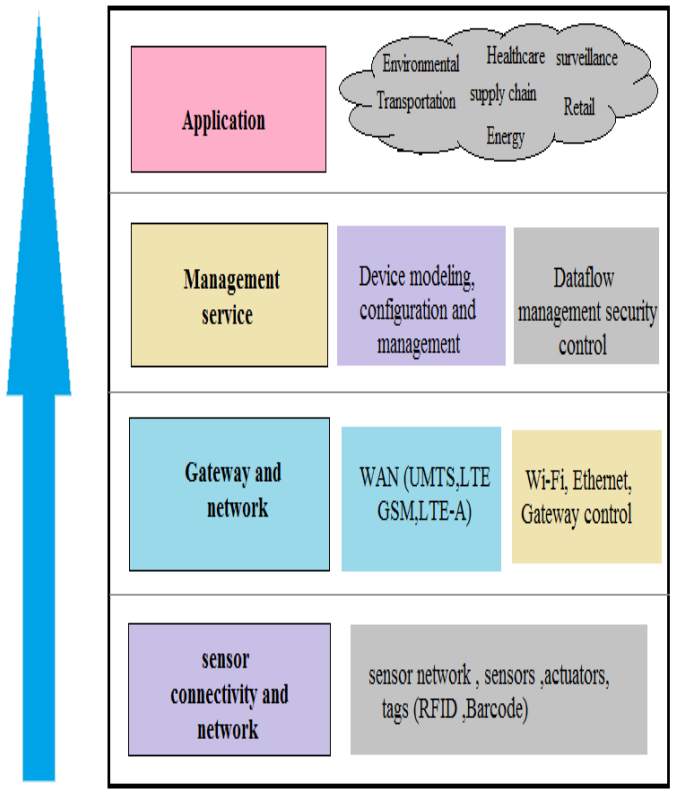

Figure1. Iot paradigm

A. Radio frequency identification

Radio Frequency Identification is based on wireless technology used for the purposes of automatic identification of electronic tags physically connected to things using an RFID reader [1]. Recently, RFID systems are broadly engaged in supply chain management, electronic payment systems, pharmacy management, library collection management, automatic toll collection, proximity cards, hospital patient care, container search within seaports and many more applications [2].

In all these applications, mechanism for the authentication of RFID tags by an RFID reader is needed to assure the legitimacy of the RFID tags when they appear in the vicinity of the reader. Because of its easy deployment RFID systems have used over a huge range of applications. Also, RFID

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

technologies have become very prominent and tangible tools in many applications such as transportation payments, identity management system, IT asset tracking, e-passports, and credit card, guarding patient safety and etc [1]. Due to these assets, a huge number of researchers have initiated to improve RFID systems currently [2-4]. With the fast expansion of RFID tags, various types of security demands have declared under RFID communication network. In various applications, the most analytical requirements considered are tag ownership transfer and grouping proofs with tag privacy, mutual authentication as well as data confidentiality [5]. Moreover, in many applications, an RFID tag can change its owner many times throughout its life cycle. Hence all information related with the tag must be passed from the old owner to the new owner. So, the new owner privacy, the old owner privacy and the authorization recovery must be well satisfied in the secure tag ownership transfer protocol [6-9].

II. AUTHENTICATION PROTOCOL

Mutual Authentication protocols are the type of computer communication or cryptographic protocol especially invented for transmission of authentication data among two items. MAP allows validating the connecting item (e.g. Client connecting to a Server) as well as validating itself to the connecting item (Server connecting to a client) by revealing the type of information required for authentication along with structure. It is the utmost significant layer of protection required for securely communicates within computer systems.

A. Elliptic curve cryptography protocol:

ECC i.e elliptic curve cryptography is a public key encryption approach. It can be used to create cryptographic keys that are very efficient and small in size.

Keys generated by ECC possess the properties of the ECE rather than the conventional method of creation that use very large prime numbers.

According to some researchers, this technology can be used with most public key encryption methods, like RSA, and Diffie-Hellman. Because it helps to setup corresponding security with less computational power and battery usage, it is seems to be broadly used method for mobile applications. ECC was developed by Certicom, a mobile e-business security provider, and was recently licensed by Hifn, a manufacturer of integrated circuitry (IC) and network security products. The use of properties and functions of elliptic curves within cryptography was first intended in 1985, by Neal Koblitz from the University of Washington, and Victor Miller at IBM. An elliptic curve is not an *ellipse*, but is drawn as a looping line crossing two axes (lines used to indicate the position of a point on a graph).

Multiplying a point on the line by a number will create another point on the line, but it is very challenging to discover what number was used, even if the initial point and the result is known. Equations that use elliptic curves hold a feature that is very beneficial for cryptography prospective: they are comparatively easy to perform, and terribly difficult to reverse [5].

a) Initialization phase:

In the initialization phase, the server generates system parameters. Server chooses a random number $PrR \in Fp$ as a reader private key and sets $PuR = PrR.P$ as its public key. Also chooses $PrT \in Fp$ as the tag private key and sets $PuT = PrT .P$ as the tags public key. Now, each tag and reader stores their key pair with the system parameters in the memory.

b) Authentication phase:

In the authentication phase we describe the interaction between tag and reader as follows:

Step 1: Reader generates a random number $r1 \in Fp$ and computes $R1 = r1.P$. Now the reader sends $R1$ to the tag.

Step 2: After receiving the $R1$, tag generates random number $t1 \in Fp$ and computes $T1 = t1.P$. *Now*, tag calculates two secret keys: $SK1T = PrT .R1$ and $SK2T = t1.R1$. Finally, the tag computes $C1 = SK1T + SK2T$.

Step 3: After receiving $(T1,C1)$, it calculate two temporary secret keys: $SK1R = r1.PuT$ and $SK2R = r1.T1$ to recover the tag encrypted secret keys. Then calculates $X = SK1R + SK2R$ and compare X to $C1$ if $X = C1$ the reader authenticates the tag to be genuine. After that it calculates $C2 = T1.PrR$

Moreover, generates new random number $r2 \in Fp$ and computes $R2 = r2.P$ to be use it for key agreement. Finally, the reader sends $C2$ and $R2$ to the tag.

Step 4: The tag compute $Y = t1.PuR$, then compare it to $C2$ if $Y = C2$ the tag authenticates the reader as a genuine.

Step 5: Both reader and tag set the key agreements between them. The tag key agreement $T\,Kag = t1.R2$ (12) and the reader key agreement $RKag = r2.T1$

B. Elliptic curve Diffie-Hellman protocol:

Elliptic curve Diffie–Hellman (ECDH) key agreement protocol is used for establishment of a secure communication channel between tag and reader. ECDH allows each party having its public-private key pair after that use it for authentication of each other and create a new key which is changeable and can be used to encrypt the communication [5]. The ECDH protocol is very easy to

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

implement. Following is the Python code that implements ECDH:

Def senderdh (prKey, creator, sdFunc):

Return sdFunc (prKey * creator)

Def receiverdh (prKey, receiveFunc):

Return prKey * receiveFunc ()

III. RELATED WORK

Want, Roy et al. [1] represented radio frequency identification technology has moved from uncertainty to popular applications that helps the supervision of constructed things and goods. RFID facilitates identification from a distance, which is not provided by earlier technologies. This paper gives introduction to the fundamentals of RFID, examine its primitive technologies and applications, and audit the threats managements will face in developing this technology. Jannati, Hoda. et al. [4] shows that Ownership transfer and grouping proof protocol both are the most essential concerns for RFID tag in numerous applications such as pharmaceutical distribution and manufacturing. Despite it, the paper present that Zuo's protocol is susceptible to de-synchronization attack and tag imitating in the existence of cheating old owner. Ahmadian, Zahra et al. [5] in this paper, the author proposed a competent ultra lightweight authentication protocol. Though it maintains the design of the existing ultra lightweight protocols, the mechanism used in it is fully different due to the use of new introduced data dependent transformation and prevention of commutable arithmetic operations and biased logical operations such as AND OR. The manufacturer of RAPP challenged that this protocol persists against de-synchronization attacks since the last messages of the protocol is sent by the reader and not by the tag. This letter challenges this assumption and shows that RAPP is vulnerable against de-synchronization attackTan, Chiu C, et al. [6] with the enlarged demand of RFID applications, various authentication techniques have been proposed to maintain security and privacy protection for clients. In this paper, the author proposes a very formative authentication protocol that offers compatible protection beyond the need for a intermediate database. We also suggest a protocol for secure search for RFID tags. We believe that as RFID applications become widespread, the ability to securely search for RFID tags will be increasingly useful.Zuo, Yanjun. et al. [7] In this paper the author proposed a number of protocols for secure and secret search for tags based on their integrity or certain fact they must fascinate. When RFID enabled systems become ubiquitous in our life, tag search becomes necessary. Surprisingly, the problem of RFID search has not been widely addressed in the literature. We analyzed the privacy and security features of the proposed tag search protocols, and concluded that our protocols provide tag identity privacy, tag source location privacy.Yong Ki, et al. [8] addressed the risk of tracking attacks in RFID networks. Our contribution is threefold:

(1) We repair three revised EC-RAC protocols of Lee, Batina and Verbauwhede and show that two of the improved authentication protocols are wide-strong privacy-preserving and one wide-weak privacy-preserving;

(2)We present the search protocol, a novel scheme which allows for privately querying a particular tag, and proof its security properties;

(3) We design a hardware architecture to demonstrate the implementation feasibility of our proposed solutions for a passive RFID tag. Due to the specific design of our authentication protocols, they can be realized with an area significantly smaller than other RFID schemes proposed in the literature, while still achieving the required security and privacy properties.

Md Endadul, et al. [9] RFID systems that have concession between reserved costs and enhanced suitability. Evolution and assets of RFID technology represents that it can be low-cost, efficient and secured solution to many universal applications. But RFID system will not interlace into human lives as far as predominating and adjustable privacy appliances are perceived. In this paper, the author recommend server less, forward secure and unattackable authentication protocol for RFID tags. This authentication protocol safeguards both tag and reader against almost all major attacks without the intervention of server. Though it is very critical to guarantee intractability and scalability simultaneously, here we are proposing a scheme to make our protocol more scalable via ownership transfer. To the best of our knowledge this feature is incorporated in the server less system for the first time in pervasive environments. One extension of RFID authentication is RFID tag searching, which has not been given much attention so far. But we firmly believe that in near future tag searching will be a significant issue RFID based pervasive systems.

Zheng, Yuanqing et al. [10] proposed utilizing compact approximations to efficiently aggregate a large volume of RFID tag information and exchange such information with a two-phase approximation protocol. By estimating the intersection of two compact approximates, the proposed two-phase compact approximation-based tag searching protocol significantly reduces the searching time compared to all possible solutions we can directly borrow from existing studies. We further introduce a scalable cardinality range estimation method that provides inexpensive input for

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

our tag searching protocol. We conduct comprehensive simulations to validate our design.

Table description: This table represents various techniques which are previously used for providing the security for RFID in the internet of things. It also represents the benefits and limitations of previously used techniques in RFID.

V. GAPS IN LITERATURE

The most of the existing technique have certain shortcomings because it has neglected things some of them are:

1. The speed of data transmission is still an challenging issue.
2. The use of ECC in IOT platform is still an open area of research.
3. The use of DNA based encryption technique is ignored by the most of the existing techniques by researchers in the field of IoT.

IV. COMPARISION TABLE

Table 1: Comparision of Various Traditional Techniques

Name of the author	Title of the paper	Technique	Benefits	Limitations
Hoda Jannati[4]	Cryptanalysis and Enhancement of a Secure Group Ownership Transfer Protocol for RFID Tags	Zuo's GOT protocol	Provides solutions to de-synchronization attack.	Zuo's protocol is vulnerable to tag imitating in the existence of cheating old owner.
Yong Ki Lee[8]	Low-Cost Untraceable Authentication Protocols for RFID	ORA protocol	The results indicate the feasibility of the protocol for passive tags, and defeat other protocols ensuring privacy and security.	NA
Md. Endadul[9]	Enhancing Privacy and Security of RFID System with Server less Authentication and Search Protocols in Pervasive Environments	server less, forward secure and untraceable authentication protocol	Results indicated that this protocol can find a particular tag effortlessly without server's interruption.	It is very challenging to guarantee scalability using this technique.
Yuanqing Zheng[10]	Fast Tag Searching Protocol for Large-Scale RFID Systems	CATS protocol and SCRE method	The results indicate that the suggested tag searching protocol is really competent in terms of time, efficiency and transmission overhead, improving suitability and scalability for massive RFID systems.	It works only on the active tags and is not implemented on the passive tags.

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

Sundaresan[14]	Secure Tag Search in RFID Systems Using Mobile Readers	128 bit pseudo random number generators and XOR encryption	Proposed protocol is efficiently implemented on passive tags and insures additional protection during all transmissions using a blind-factor.	NA
HangRok Lee[15]	The Tag Authentication Scheme using Self-Shrinking Generator on RFID System	SSG algorithm	The proposed scheme only requires the 64byte memory and is very suitable and practical for passive tag.	SSG is vulnerable to security attacks like bdd attack and is implemented only on the passive tags.
Joyashree Bag[16]	VLSI Implementation of a Key Distribution Server Based Data Security Scheme for RFID System	KDSS and PCA rule	Useful in remote places to classify unique item or lead to right route	NA
M. Ramakrishna[17]	Mutual Authentication Protocol for RFID Security using NFSR	XOR operation and NFSR	Security analysis indicates that this protocol is offering diverse privacy features and protection from different kinds of attacks such as replay tag, tag anonymity, mutual authentication reader privacy, transfer secrecy, tag, location protection etc	NA

VI. CONCLUSION

Radio frequency identification technology developed in many applications, such as transportation payments, identity management system, IT asset tracking, e-passports, and credit card. These applications demand security on different levels based on their demands and capacity which may accomplish by authentication protocols. In this paper we discusses the comparison on various encryption techniques and protocols that attains set of security features likes mutual authentication, anonymity, scalability, intractability and confidentiality. By conducting the survey there are some issues in performance while using RFID authentication protocol based on elliptic curve cryptography. So to improve the performance we will evaluate ECC based encryption techniques that enhances the computational speed.

REFERENCES

[1] Want, Roy. "An introduction to RFID technology." IEEE pervasive computing 5.1 (2006): 25-33.

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

[2] Amjad ali alarm, Firdous Kausar. “A secure ECC-based RFID mutual authentication Protocol for internet of things.” J Supercomput DOI 10.1007/s11227-016-1861-1

[3] Miles, Stephen B., Sanjay E. Sarma, and John R. Williams, eds. RFID technology and applications. Vol. 1. Cambridge: Cambridge University Press, 2008.

[4] Jannati, Hoda, and Abolfazl Falahati. "Cryptanalysis and enhancement of a secure group ownership transfer protocol for RFID tags." Global Security, Safety and Sustainability & e-Democracy. Springer Berlin Heidelberg, 2012. 186-193.

[5] Ahmadian, Zahra, Mahmoud Salmasizadeh, and Mohammad Reza Aref. "Desynchronization attack on RAPP ultra lightweight authentication protocol." Information processing letters 113.7 (2013): 205-209.

[6] Tan, Chiu C., Bo Sheng, and Qun Li. "Secure and server less RFID authentication and search protocols." IEEE Transactions on Wireless Communications 7.4 (2008): 1400-1407.

[7] Zuo, Yanjun. "Secure and private search protocols for RFID systems." Information Systems Frontiers 12.5 (2010): 507-519.

[8] Lee, Yong Ki, et al. "Low-cost untraceable authentication protocols for RFID." Proceedings of the third ACM conference on Wireless network security. ACM, 2010.

[9] Hoque, Md Endadul, et al. "Enhancing privacy and security of RFID system with server less authentication and search protocols in pervasive environments." Wireless personal communications 55.1 (2010): 65-79.

[10] Zheng, Yuanqing, and Mo Li. "Fast tag searching protocol for large-scale RFID systems." IEEE/ACM Transactions on Networking (TON) 21.3 (2013): 924-934.

[11] Chen, Min, et al. "An efficient tag search protocol in large-scale RFID systems with noisy channel." IEEE/ACM Transactions on Networking (TON) 24.2 (2016): 703-716.

[12] Piramuthu, Selwyn. "Vulnerabilities of RFID Protocols proposed in ISF." Information Systems Frontiers 14.3 (2012): 647-651.

[13] Safkhani, Masoumeh, et al. "On the security of Tan et al. server less RFID authentication and search protocols." International Workshop on Radio Frequency Identification: Security and Privacy Issues. Springer Berlin Heidelberg, 2012.

[14] Sundaresan, Saravanan, et al. "Secure tag search in RFID systems using mobile readers." IEEE Transactions on Dependable and Secure Computing 12.2 (2015): 230-242.

[15] Lee, HangRok, and DoWon Hong. "The tag authentication scheme using self-shrinking generator on RFID system." Transactions on Engineering, Computing, and Technology 18 (2006): 52-57.

[16] Joyashree Bag, et al.” VLSI Implementation of a Key Distribution Server based Data Security Scheme for RFID system.” 2015 Fifth International Conference on Advanced Computing & Communication Technologies

[17] T. Suresh, M. Ramakrishna, et al. “Mutual Authentication Protocol for RFID Security using NFSR” 2015 IEEE.