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

**Er. Rawinderjit singh [1], Er. Sanjeev Mahajan[2]**

*[1] M.Tech Scholar, Department of Computer Science & Engineering,
Beant College of Engineering & Technology,
Gurdaspur*
*[2] Associate Professor, Department of Computer Science & Engineering,
Beant College of Engineering & Technology, Gurdaspur*

***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.**

## 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.

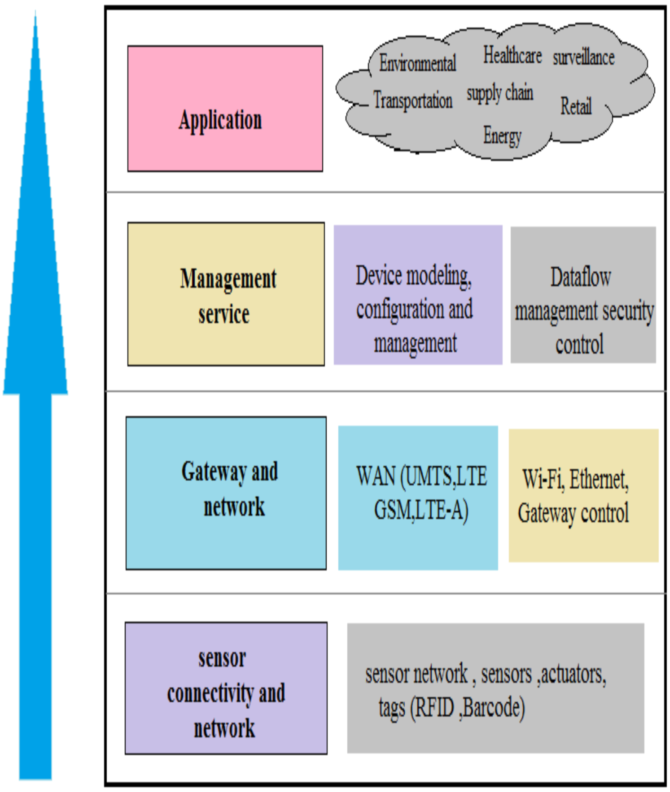
Application
Environmental
Healthcare
surveillance
Transportation
supply chain
Retail
Energy
Management service
Device modeling, configuration and management
Dataflow management security control
Gateway and network
WAN (UMTS,LTE GSM,LTE-A)
Wi-Fi, Ethernet, Gateway control
sensor connectivity and network
sensor network , sensors ,actuators, tags (RFID ,Barcode)

Figure1. Iot paradigm

## Radio frequency identification

Radio Frequency Identification is based on wireless technology used for the applications of intelligent recognition of electric labels actually attached to points having an RFID audience [1]. Lately, RFID techniques are commonly involved in source cycle administration, electric cost techniques, drugstore administration, selection series administration, intelligent cost series, area cards, clinic individual treatment, pot research within seaports and a lot more programs [2]. In every one of these programs, process for the validation of RFID labels by an RFID audience is necessary to promise the legitimacy of the RFID labels if they come in the location of the reader. Also, RFID systems are becoming really distinguished and real methods in lots of programs such as for instance transport funds, identification administration program, IT advantage monitoring, e-passports, and charge card, guarding individual security and an such like [1]. As a result of these resources, and endless choice of scientists have started to boost RFID techniques presently [2-4]. With the rapidly growth of RFID labels, numerous kinds of protection needs have reported below RFID transmission network. In several programs, probably the most logical demands regarded are label possession move and collection proofs with label solitude, common validation in addition to information confidentiality [5]. Moreover, in lots of programs, an RFID label can alter their operator often times for the duration of their living cycle. Thus all data connected with the label should be transferred from the previous operator to the newest 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].

### 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.

## 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 portable applications. ECC was manufactured by Certicom, a portable e-business protection company, and was lately registered by Hifn, a supplier of incorporated circuitry (IC) and system protection products.

## 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 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 ()
```

### 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.

Tan, Chiu C, et al. [6] proposed a really formative verification project that gives suitable security beyond the requirement for a advanced database. We also recommend a project for protected look for RFID tags. We feel that as RFID purposes become common, the capacity to solidly look for RFID labels is likely to be significantly useful.

Zuo, Yanjun. et al. [7] 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.

## COMPARISON TABLE

### Table 1: Comparison of Various Traditional Techniques

| Name of the author | Technique | Benefits | Limitations |
|---|---|---|---|
| Hoda Jannati [4] | 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] | 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] | 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] | 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. |
| Sundaresan[14] | 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] | SSG algorithm | The proposed scheme only requires the 64byte memory and is very suitable and ractical for passive tag. | SSG is vulnerable to security attacks like bdd attack and is implemented only on the passive tags. |
| Joyashree Bag[16] | KDSS and PCA rule | Useful in remote places to classify unique item or lead to right route | NA |
| M. Ramakrishna[17] | 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 |

**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.

## 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 image encryption is still an challenging issue.
2. The use of optical domain is ignored by the most of the existing researchers in the field of IoT.
3. The use of DNA in optical domain techniques is still an open area of research.

## 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.
[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

## BIOGRAPHIES

Er. Rawinderjit Singh
M Tech Scholar, Department of CSE, BCET, Gurdaspur, Punjab, INDIA – 143521

Er. Sanjeev Mahajan
Associate Professor, Department of CSE, BCET, Gurdaspur, Punjab, INDIA - 143521