LITERATURE REVIEW

1] Cristina Hurjui, Adrian Graur, (2010), In this paper four protocols based updating on the tag’s identifiers by means of RFID readers will be compared, in order to carry out an analysis over the jeopardizing points

Design Procedure:- Four protocols based updating on the tag’s identifiers by means of RFID readers will be compared.

Henrici and Muller’s protocol the RFID transponder needs the storing of an identifier ID and two variables $k$ and $k_{last}$. The transponder contains its current ID, the number $k$ of session and $k_{last}$ equal to $k$. As conclusion, an adversary can always detect a tag between two correct identifications, which are carried out.

Golle, Jakobsson, Juels and Syverson’s protocol is based on the concept of universal re-encryption this protocol is not designed so as to face simple attacks of interception. A tag sends in its second message what it received in a previous execution process, meaning its third message. Thus, a potential adversary can detect that tag by means of an interception method.

Saito, Ryou and Sakurai’s protocol proposed two RFID protocols, RFID privacy protocol with one check. Attack based upon private keys, Potential attacks relying on desynchronizing the database of the RFID system

Juel’s protocol based upon XOR, assigns the storing of pseudonyms, denoted as a list under the form $\alpha_1,...,\alpha_k$. Every time a tag is interrogated by a reader, this will use a new pseudonym, by a cyclical method at the beginning of the list and after $k$ successive identifications. One might notice that only few pseudonyms can be stored, since the memory of tags is limited.

2] Damith C. Ranasinghe, Daniel W. Engels, Peter H. Cole,(2004), RFID that too with low cost are increasingly being deployed in industry and commerce This paper presents proposals on feasible security mechanisms for low cost RFID systems and analyses them from both security and privacy points of view.

The MAC implementation takes a very simple approach This mechanism does raise the difficulty level for forgers as the process of eavesdropping and creation of fake labels is made more difficult, however it does not provide privacy as the ID code embedded in the chip will breach anonymity and location privacy. There is also the risk of the key, which is common to many
labels, becoming known. TEA is an encryption algorithm designed for simplicity and ease of implementation. Despite the simplicity and the ease of implementation of the cipher, the level of security or its vulnerability to attacks are still not very clear.

The security of the system depends on the difficulty of replicating a PUF circuit and on the difficulty of modeling the PUF circuit successfully. This is not a simple process and is therefore an adequate deterrent depending on the value of the article being authenticated by the reader.

Re-encryption offers a novel perspective on achieving these goals. Re-encryption provides anonymity by never transmitting a predictable response, an encrypted forward link and also allows the authentication of a reader and a label. A simple approach to developing an authentication scheme and providing a secure forward link can be designed by using a single secret (K). Once a reader has uniquely identified a label, a reader may use that information to discover a secret K, and two time stamps

3] Lan Zhang, Huaibei Zhou2, Ruoshan Kong, Fan Yang,(2005),This paper briefly presents the current solutions to security and privacy of RFID application system. After that an improved approach is proposed which is based on random number assisting and symmetric encryption. Then, the paper analyzes it from both security and privacy points of view. Finally, it gets the conclusion that this scheme will prevent tracking, spoofing and attacking by adversaries effectively.

4] Xingxin(Grace) Gao, Zhe(Alex) Xiang, Hao Wang, Jun Shen, Jian Huang, Song Song,(2004), A new approach is then proposed, which exploits randomized read access control and thus prevents hostile tracking and man-in-the-middle attack. In addition, compared with current schemes that achieve the similar security level, the proposed approach dramatically decreases the computation load.

5] R.K. Pateriya, Sangeeta Sharma,(2011),This paper reviews the approaches which had been proposed by scientists for privacy protection and integrity assurance in RFID systems, and treats the social and technical context of their work.
6] Wang Qinghua, Xiong Xiaozhong, Tian Wenhao, He Liang,(2011),Introduces the data security and privacy problems existing in RFID system from the perspectives of label, network and data security etc. then, discusses the solutions for the existing security and privacy problems from the perspectives of physical security mechanism and protocol of RFID system.

7] John Ayoade,( 2004),In this paper, we are trying to weigh the two issues, importance of RFID system and the RFID security implications. Having done that, we are recommending our idea called APF (Authentication Processing Framework) as a good method to overcome the above mentioned problem.

8] Mala Mitra,(2008),Apart from data leakage, the technology suffers from tracking of object and cloning of tag problems. Here a review has been done on the existing solutions. A new algorithm with scalable privacy has been proposed here.

9] Herdawatie Bt Abdul Kadir, Mohd Helmy Abd. Wahab and Siti Nurul qmaria Bt Mohd Kanafiah,(2009),The application of RFID Matrix Card system as a boarding school students monitoring system (E-ID) were purposed to improve school management system and to monitor interest group movement. The RFID tags enable school management to track the students movements in and out of the hostel.

10] Mohd Faizal Mubarak, Jamalul-lail Ab Manan , Saadiah Yahya,(2011), It propose an overall approach that considers security, trust and privacy (STP) together We propose to use lightweight based encryption subsystem to handle security, trusted computing based subsystem to provide trust and integrity verifications and privacy enhanced system (anonymizer) to solve privacy issues for RFID system.

11] Hap Nguyen,(2005 ),An anti hi-jacker system for use in association with a transportation conveyenence having an engine or motor system. It includes a RFID tag associated with an authorized user of the transportation and a receiver to read signal transmitted by the RFID tag.
12] Tuttle; John R.,(2004). A radio frequency identification (REID) device may include a first, thin, flexible sheet, an antenna, and an integrated circuit. A surface portion of the first sheet may be affixed to a second, thin, flexible sheet to form a thin, flexible label. Such a label may be affixed to an article for tracking by an interrogation system.


14] Stephan Haller,(2004). The RFID system are configured to receive signals from RFID interrogators. the controller process the signal from the RFID and provide data to the application.

15] Teruhisa Ninomiya,(2005). This paper presents an invention as to provide a carrier sensing method capable of carrier sensing even then the difference with respect to the carrier frequency by other system is close to ‘0’ an RFID transceiver device and RFID system employing this method.

16] Jung-Hyun Oh, Hyun-Seok Kim and Jin-Young Choi,(2007). In this paper, we proposed a security protocol which is based on one time pad scheme using random nonce and shared secret values. The protocol satisfies the security requirements and the low-cost implementation requirement.

17] He Lei, Gan Yong, Cai Zeng-yu, Li Na-na,(2009). Many researchers proposed some lightweight authentication protocols which only use lightweight operations, such as hash function, XOR etc. In this paper, we analyze the security of protocols respectively proposed by Li et al and Chien et al.

18] Chun-Te Chen, Kun-Lin Lee, Ying-Chieh Wu, and Kun-De Lin,(2006). This paper proposes a key management to distribute the access key and the encryption/decryption keys based on the Role-base Access Control method. With the proposed management framework, it not only simplifies the procedure of access RFID, but also selects proper privilege to user. The kind of
privilege is chosen by key manager and key manager had divided employees into six roles according to their task characters.

19] Shuai Shao, Guoai Xu, Yanfei Liu,( 2006),This paper presents a new efficient RFID authentication scheme with strong security and privacy. The proposed scheme is suitable for managing a large number of tags, for taking constant time to authenticate a tag by using hash chain.

20] Ali N M Noman, Sk. Md. Mizanur Rahman and Carlisle Adams,(2011),we propose a complete tamper detection solution for low cost RFID tags; this solution has the potential to improve the security and usability of low-cost RFID tags. Moreover,we also conducted a thorough analysis of this proposed solution to show that it conforms to the EPC-C1G2 specification. Last, but not least, it also justifies why the proposed solution is better than the existing tamper detection solutions.