International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

Analysis of lightweight cryptographic algorithm for RFID smart card Reader

Apoorva N[1] , Karthik C Shekar[2], Prajakta M[3]

[12]Student, [3]Professor,

Dept of Information Science and Engineering ,The National Institute of Engineering, Mysore,India

---

Abstract – *Radio Frequency Identification (RFID) is a new emerging technology that is widely used and deployed for object tracking and monitoring, ticketing, supply-chain management, contactless payment, etc. In today's digital world digitization has lot of importance. Cashless transaction or cashless payments have become a popular trend and there is a need for the digital data transactions to be more secured. These cashless payments are already there in many places but here in this paper we are concentrating on data security in IoT based environment we are coming up with the "lightweight security protocol" for encryption and decryption of data without exchanging the security keys. Firstly we compare among the existing system. Later we describe the issues and challenges in these system. Finally we analyze the lightweight cryptographic algorithm is efficient for RFID smart card reader*

Key Words: **IoT, protocol, cryptography**

1.INTRODUCTION

In the past decades, with the fast emerging technology of wireless communication techniques and mobile services, numerous commercial systems and e-commerce applications have been proposed for users to communicate, collaborate and share their information with other people. However, owing to the insecure nature of wireless channels, many security issues, such as data leakage and personal data privacy, need to be carefully addressed when a wireless communication system is being developed and used.

These days, cashless transaction have become a popular trend and there is a need for the digital data transactions to be more secured. These cashless payments are already existing but since we are concentrating on data security in IoT based environment we need a protocol with less computational overhead, high efficiency, scalable, reliable algorithm. RFID as the core technology of IoT, the security issues have emerged widely.

In the present scenario, there is a necessity to develop lightweight RFID security protocols for such low cost and low computation capability tags. One such algorithm suitable for this environment is lightweight cryptographic protocol called Trusted-third-party-based High-efficient Multi-Key Exchange Protocol (THMEP for short).

1.1 Security threats of existing system

The existing system has two main security issues. One of them is the security of the RFID system which includes the RFID tag and RFID reader. Another is the communication security for the communication between RFID tag and RFID reader as well as between the RFID reader and database. These security threats are discussed in detail in TABLE 1

TABLE I. THE SECURITY THREATS AND THEIR

REASONS

Security threats		The reason
RFID system	Abuse of tags(tag cloning)	The weakness of tags
	Reader risks	The weakness of readers
	Personal privacy leak	traceability and identification of the tags
	Signal interference	Interference between the low adjacent band
Communication security treats	Wireless communication risks(search, intercept, monitor, and jam wireless communication signals)	the openness of the wireless signals
	wired communication risks	The openness of the internet
	Denial of Service (DOS)	Malicious attackers

1.2 Security attacks

Eavesdropping is the method of monitoring all the communication between the tag and the reader and thereby obtaining the information contained in the tag .Such attacks are to be avoided to maintain confidentiality in the system.

Spoofing is the method of posing as a normal user having a genuine label. Spoofing is usually carried out by replacing the tag of an expensive item with a fake tag or by using a fake tag for a valid item**.**

Denial of Service Denial of Service or DoS is one of the most common attacks carried out on any security system. In an RFID system, a DOS attack is initiated by introducing a large number of fake tags for the reader to identify thus using up most of its resources. Another way in which a DOS attack is carried out is by corrupting or destroying a large number of valid RFID tags. This is a type of brute force attack which has raised huge security concerns.

Man in the middle attack is a simple way of misleading the RFID reader. This is done by modifying the response sent from the tag to the reader. This is done by continuously monitoring the traffic between the tag and the reader and then modifying some of the data before it is transmitted to the reader.

Replay Attack **:** This does not affect the integrity of the data but the confidentiality is compromised. The attacker simply eavesdrops on the communication between the tag and the reader. The response of the tag is first captured by the attacker and then retransmitted back to the reader.

Data loss This is caused by improper maintenance of the RFID system. Data loss mainly occurs when there is no backup power or backup storage. In such cases a power interruption or database desynchronization can cause data loss. The data may also be hijacked by an adversary.

2. Light weight cryptographic solution for RFID smart card reader

Devices in internet of things (IoT) are frequently

i. The source constrained and

ii. Deployed in unmonitored, physically insecure environments.

Securing data of these devices requires tractable cryptographic protocols, as well as cost effective tamper resistant solutions. We propose "Lightweight security key exchange protocol" for sending data from IoT to the target with less computation and more security

Due to security issues in the existing system we need a less computational overhead protocol. one such lightweight cryptographic protocol is Trusted-third-party-based High-efficient Multi-key Exchange Protocol (THMEP for short), is proposed to provide users with a secure and efficient protocol, which employs the elliptic curve cryptography, a two-dimensional operation, and a current time encryption key, to exchange their session keys. The proposed protocol not only effectively hides important encryption parameters, but also achieves fully mutual authentication between a user and his/her trusted server.

Our security analysis shows that the THMEP has a higher security level than those of three state-of-the-art approaches, including replay attack prevention, eavesdropping attack prevention, and forgery attack prevention

3. CONCLUSIONS

Due to computational overheads in the existing system and static key exchange. These existing systems are more prone to many attacks like forgery, eavesdropping, replay attacks .In today's world cashless transactions plays a enormous role.Our system with the THMEP enhances the computational performance and security level of the key exchange process in mobile communication. Comparing with previous studies, the THMEP has lower computation and communication costs and provides 40 session keys. The processing speed of the THMEP is 3.78 times faster than that of the 3MPAKE when the key length is 1024 bits. This protocol efficiently hides all the parameters

Hence traditional heavy weight algorithms are not apt for IoT due to their constrained environment. Hence, alternate lightweight cryptography solutions symmetric as well as asymmetric can be used.

REFERENCES

[1] A. Kahate, "Cryptography and Network Security",TMH-2003

[2] U. Varshney and R. Vetter, "Mobile Commerce: Framework,Applications and Networking Support," Journal of Mobile Networks andApplications, vol. 7, no. 3, pp. 185–198, June 2002.

[3] TTP based High-efficient Multi-Key Exchange Protocol
IEEE, Fang-Yie Leu, Member, IEEE, Ilsun You, Senior Member, IEEE. Kun-Lin Tsai, Member, IEEE, Yi-Li Huang, Member

[4] Cryptography and Network Security, Behrooz Forouzan, SIE, 2nd Edition, McGraw-Hill.

[5] Cryptography and Network Security: Principles and Practice; Fifth Edition, By William Stallings, Prentice Hall.