ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 2, Issue 6, June 2014

Implementing In-Cloud Security for effecting secured communication between Intelligent Tags and Mobile Devices

Dr. JKRSastry, Dr. A. VinyaBabu

Department of Computer Science and Engineering, KL University, Vijayawada, India

Department of Computer Science and Engineering, JNTU Hyderabad, India

Abstract: Intelligent Tags communicates with mobile devices using one of the wireless communication protocols for transmitting the environment related to Mobile devices which may be situated at remote locations. The data transmitted to the mobile devices is quite sensitive and therefore must be secured. Building security mechanisms with the Tags will affect the design of the tags especially effecting the response time and throughput. More intelligence has to be built into Tags if attacking is to be sensed and then enforcing the counter attack mechanism in which the response time and throughput may temporarily get effected because security enforcement is under taken only when attacking takes place. However there should be in process implementation of security enforcement without effecting the response time and throughput. The paper presents a method of enforcing in-cloud security by using a PC in the neighborhood of a PC.

Keywords: Intelligent Tags, Wireless communication, security enforcement within embedded systems, attacking and counter attacking, in-cloud security

I. INTRODUCTION

Implementation of various intelligent aspects on the TAG side requires that the Tags communicate with the HOST (Mobile phone) on continuous basis exchanging every important information. As the TAGS become more intelligent, they deal with very sensitive information and the same is communicated to the user of the TAGS through mobile phone interface. It is possible that the intruders can attack the communications that takes place between the TAG and the mobile device.

The TAGS must be protected from attacking without loss of response time and throughput. Securing an embedded system is a challenge as the embedded systems are low in resources. The communication between the TAG and the HOST is actually venerable as the communication takes place through wireless technologies which includes Bluetooth Wi-Fi, NFC etc.

The penetration into the communication taking place between the HOST and the TARGET is dependent on the type of communication protocol used. When Bluetooth is used, the communication can be attacked through various means which include Blue Jacking, Blue sniffing etc. Several counter measures are also in vogue that makes the communication secured.

Implementing features into the embedded applications permanently resident along with the application code will add heavy overhead and effects the response time and throughput drastically and at the same time it may lead to effecting the real time requirements of the embedded systems.

One way of implementing the security without effecting the response time is to sense that attacking is taking place and then bring in the securing features to be effected so that attacks can be counter attacked effectively. In this case the response time and the throughput will suffer temporarily till the time the attacking is in progress. When the attacking ceases, the securing feature is withdrawn and the normal operation is continued. This method however is ineffective when the attacking is severe and continuous as the presence of the same requires running of the security related infrastructure on continuous basis leading heavy overhead on the requirement of resources and the need for the embedded system to operate in degraded manner if the application design permits operating the embedded system at low levels of operation

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 2, Issue 6, June 2014

Thus, there is a need for developing intelligence into the TAG for securing the communication between the TAG and the mobile device considering that the attacking is continuous and that the counter attacking mechanisms must be in process without the need to add too many resource or upgrading the ES resources which yield higher level of performance than required for original application.

A specific type of attack requires a set of related securing mechanisms. There can be many types of attacks and their corresponding counter attacking mechanisms. Building in-process counter attacking mechanisms for all possible types of attacks is cumbersome and requires huge amount of resources. To avoid this there should be process that recognizes an attack and enforce the security through in-cloud mechanism. In this paper In-cloud security method has been proposed for enforcing the security that is just relevant to the type of attack that is initiated by the hacker

II. RELATED WORK

Many methods have been invented in the past for securing the stand alone embedded systems considering various attacks and counter attacks which can be classified into the categories which include timing, electromagnetic analysis, power analysis and fault injections. Many attacking and counter attacking methods have been proposed and implemented in the past for securing the stand alone systems [**19**], [**11**], [12], [18], [**13**] [**14**], [**15**], [**16**], [**17**].Several authors have addressed the issue of securing the communication between the TAG and the HOST considering the communication protocols and the devices.

Dieter Hutter [1] - suggested a model that includes transmission of a randomly chosen key by encrypting the key value with the Hash function computations i.e. h (key). Only the reader with exact corresponding key will be able to respond to a TAG and then only the specific TAG will transmit the ID value of it. But in his proposal the ID value is static. So, there is maximum chance for the adversary to trace that particular TAG and to perform eavesdropping on the communication between reader and TAG. Later he suggested an advanced version of his previous protocol by implementing the randomness to the key value. But it was not providing forward security for the communication between them and is vulnerable to replay attacks.

Miyako Ohkubo [2] - used Hash chains to propose a protocol for securing communication between a TAG and a HOST. It mainly concentrated on the implementation of forward security such that the data sent by the TAG is to be secured even when a function within the TAG accidentally reveals the information handled by it. But the method has not been succeeded because of the computational overhead involved in the calculation of the hash chains at the back-end database.

Dirk Henrici[3] - suggested the usage of one way hash functions such that the location secrecy of a TAG can be enhanced by changing the identifier values of that TAG for every reading instant by using a simple message exchange. The adversary will be successful in making a TAG undetectable to get access to communicate with its reader by blocking the communication using denial of service attacks (DOS) or by employing the Kill TAG approach.

Tassos Demetrio [4] - proposed a protocol which ensures privacy and resistance to TAG cloning. In this scheme, the secret key value is shared between the TAG and the reader such that it will be modified for successful successive identification. In addition, the authentication is verified on both reader and TAG sides using a single secret key. But tracking of TAG is still possible because a value transmitted by the Tags will be remained static between two successful identifications. Hence, it is vulnerable to a database de-synchronization attack.

Young Ju Hwang [5**]** - suggested an authentication protocol which consists of two one way hash functions that can be used to provide privacy for low cost RFID Tags whose constraints are, low power sources, and computational capabilities. It is framed as Low Cost Authentication Protocol (LCAP). These types of low computational supporting Tags are vulnerable to replay attacks, database de-synchronization attacks and tracking attacks.

David Molnar et[6]- suggested a model in which a TAG and a database should have to share two secret values called identifier of TAG and secret key. These values along with two words, used especially for computations generated by the reader and the TAG are fed into a pseudorandom function. This scheme ensures privacy and protection against tracking attacks but does not offer forward security.

Xingxin GAO[7] - suggested a scheme which is used to exploit randomized access control and that should be able to prevent hostile tracking and MIM (Man in the middle) attacks. This scheme offers limited computational overhead and it is useful for systems with several RFID Tags. But it does not offer forward security and is vulnerable to replay attacks.

Dominic [8] - suggested that when two wireless devices are intended to communicate with each other using various communication standards like Bluetooth, Wi-Fi, NFC etc, a pairing procedure is necessary to ensure the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 2, Issue 6, June 2014

privacy of a system. This can be achieved by using necessary encryption at link layer level. But this method will not yield good results to the user and is vulnerable while attacker performs eavesdropping on the pairing procedure.

Sastry [9] [10] have proposed a security mechanism that implements the intelligence to sense the situations of attacking and bring into the scope, the counter attacking mechanisms. The counter attacking mechanisms must only come into play at the time when an attack is initiated. The counter attacking mechanisms are not to be inbuilt as in-stream procedures as it effects the response time and as such both the TAG and the Mobile devices are short in resources and also the components of embedded solution are basically slow devices and the permanent residence and inline execution of any of the code actually hampers the design parameters of the embedded systems. An architecture that caters for the enforcing security when happens has also been proposed by them.

Hanunah Othman [21]have explained that more of hardware and software must be added to the mobile devices , as more and more diversified functions are added to the mobile devices. Existing software built into mobile devices is vulnerable and can easily be attacked as not much of security infrastructure is available to protect the software on the mobile device. They have proposed Trusted Computing environment in order to develop an open security platform that can be used in all industrial fields and solve existing software security vulnerabilities via a hardware security module**.** The solution proposed is limited to the trusted environment created in the neighborhood of mobile device

Sameer Hasan [22]have proposed and implemented a non-server (that is, Peer to Peer) architecture public key cryptography to secure the mobile communications. The proposed implementation of public key cryptography provided confidentiality, authentication, integrity and non-repudiation security services needed for mobile communication. They proposed that compared with server based architecture, non-server based architecture has lower risk and the security has been improved, to avoid many kinds of attacks. In this finding, much of the overhead is added to the Mobile phone making it literally infeasible for implementation.

SeifedineKadr[23]has proposed a technique for securing mobile communications based on the usage of the Fingerprint to identify both the speaker and the sender. This technique is simple, requires less calculation than other public/private key techniques, assures more authenticity than digital signature, and eliminates the need for a third party. Moreover, when applied to mobile phones, they proposed that this technique resists any forge imposed by another party. This security feature is limited to authentication of the user to use the mobile phone.

DijiangHuang [24**]** has used weblets to link the cloud services and mobile devices. They proposed that a weblet execution can take place on the mobile device, or migrated to the cloud. This approach dynamically augmented the capabilities of a mobile device including computation power, storage, and network bandwidth. This approach recommended that one or more weblets are controlled by the application root, which is the part of the application that provides the user interfaces and issues requests to the weblets. This process has the week links that while the mobile device is in communication using web the web links could be exposed there by leaving weak links.

Hoang T. Dinh [25]discussed that as mobile devices are constrained in their processing and power. Protecting them from the threats is more difficult than that for resourceful device It is impossible to keep running the virus detection software on mobile devices. They proposed architecture that locates threat detection capabilities within cloud computing platform. The architecture proposed by them heavily adds application components on the mobile device. Primarily the approach proposed by them helps in detecting malware. The platform consists of host agent on the mobile device and network service components & security infrastructure located on cloud computing platform.

Satish Narayana Sriram [26]mainly addressed the details and issues in providing secured communication and access control for the mobile web service provisioning domain. They have r discussed details of secure communication and proposed the distributed semantics-based authorization mechanism. For the trusted and distributed management of access control to protect mobile web services, they proposed to use Semantics-Based Access Control (SBAC). SBAC is the result of adoption of the Semantic Web vision and standards to the access control research and development field. Administration and enforcement of access control policies based on semantics of web services, clients, mediating actors and domain concepts comprise the most suitable approach to handle openness, dynamics, mobility, heterogeneity, distributed nature of environments that are involved in the mobile web service provisioning. The Mobile host in the proposed system creates some extra load caused by the security mechanisms will have some serious impedances on the battery life of the devices and smart phone's basic purposes like making normal telephone calls.

Anand Raghu Nathan [27]has proposed secure hardware/software platform architecture for several security concerns in mobile applications. Security processing refers to computations that need to be performed specifically for the purpose of security. The computational requirements of security processing place a significant burden on the embedded processors used in mobile appliances, and can lead to significant degradations in battery life. They proposed

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 2, Issue 6, June 2014

the system to have embedded processor enhancements for securing processing, Cryptographic hardware accelerators and Programmable security protocol engines.Sastry [28] have proposed architecture for enforcing security within mobile phone using clouds which supports the entire infrastructure required for enforcing security within mobile phone which is a kind of embedded system by it.

III. ENFORCING IN-CLOUD SECURITY

A cloud is established with the entire infrastructure required for implementing security related mechanisms.The cloud computing layer will provide all the interfaces required for establishing the communication between the mobile device and cloud computing platform. The mobile devices before communicating a message/data/file etc., to another device, shall send the same to locally tightly coupled cloud computing platform through communication interface which is established either through a Wi-Fi or Bluetooth depending on the distance at which the mobile device is located.

The cloud computing software, will invoke the functions in the middleware based on the security service requested by the mobile device, so that the requested service is rendered and the secured Data/Message/ File etc., is sent back to the mobile device. The mobile device intern transmits the same to the receiving mobile device through usage of regular communication network. The receiving mobile device in-turn will do the reversal of the operations carried by transmitting mobile device so that data / message / file etc., are unsecured and then used for regular processing. The architecture that implements the in-cloud security is shown in the **Figure 1.**

It can be seen from the figure I that all the service providers will individually register with the cloud computing software there by providing uniqueness in providing the services to the users. The paths that are traced for effecting different types of communication between mobile devices and the vulnerabilities that existed at different locations and the way the vulnerabilities are attacked and counter attacked have been explained [28]. Different kinds of counter attacking mechanisms have been proposed based on the vulnerability of attacking. The venerability has been established when a message is passed or an email is communicated, or a file transfer is affected or a mobile commerce related transaction has been effected. The process that needs to be undertaken for affecting the security based on the location of venerability has also been presented.

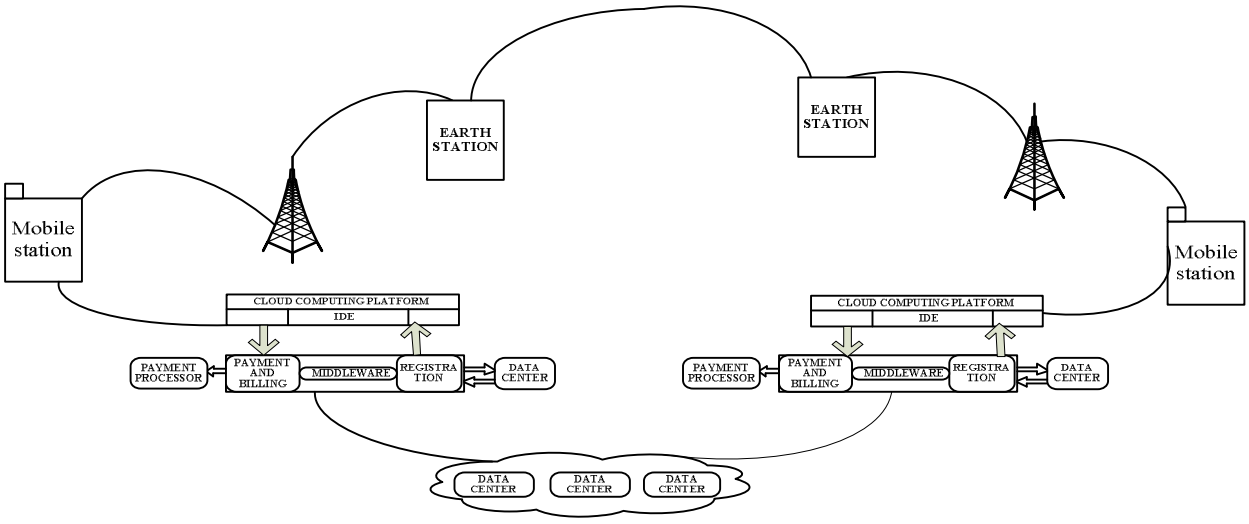

Figure1 Overall architecture for enforcing Mobile security

In similar lines of effecting secured communication as shown in the figure, the communication is effected between a Mobile phone and a Tag, using the architecture shown in the **Figure 2.**A cloud infrastructure is used to effect the communication between a Tag and mobile device. The messages / data communicated between the Mobile device and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 2, Issue 6, June 2014

the Tag is secured through the clod. The Cloud supports all the services required for ensuring security of the messages flowing across the mobile device and the Tag. Thus the TAG and the mobile devices are relived of the overhead required for ensuring the security has been shifted to the cloud. The cloud shall have both Bluetooth and Wi-Fi interface using which the Mobile and the Tag can communicate with the cloud.

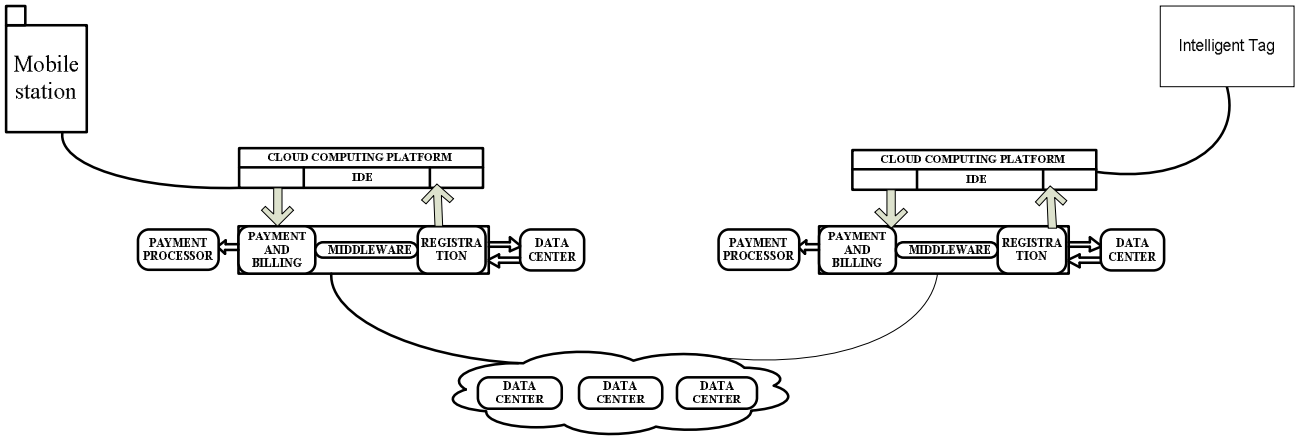

Figure 2 Effecting secured communication through in-clouds

IV. SENSING ATTACKING AND EFFECTING THE SECURITY

In the aspect of providing security for an Intelligent Tag, the key requirements on both sides i.e. on the host side and the target side are Bluetooth, Wi-Fi communication modules. As the Tag has to be made intelligent to perform functions like identifying its own location, alerting the master about an event occurring in its vicinity, sensing tampering with its own etc, the Tags should communicate with the host by using the available interface at either end for transmitting the data from the Tag side and for receiving commands from the host. **Figure 3** explains the communication architecture to facilitate communication between the communicating devices.

The communication interfaces that are mainly needed to establish communication between a Tag and a Remote Host (Mobile Device) are Bluetooth and Wi-Fi modules. As the devices on either side have to communicate using the available and active interfaces, there is need for implementing the exchange of the protocol i.e., from Bluetooth to Wi-Fi and Wi-Fi to Bluetooth. This can be achieved by introducing a protocol converter in between Bluetooth and Wi-Fi interfaces in the communication architecture.. Using this Protocol Converter, if the communication interfaces available on the tag side and mobile device side are Bluetooth and Wi-Fi respectively, then the data needed to be transmitted to mobile device will be converted from Bluetooth protocol to Wi-Fi protocol by sending via protocol converter. In this way the conversion of protocol from Wi-Fi to Bluetooth will be implemented.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 6, June 2014

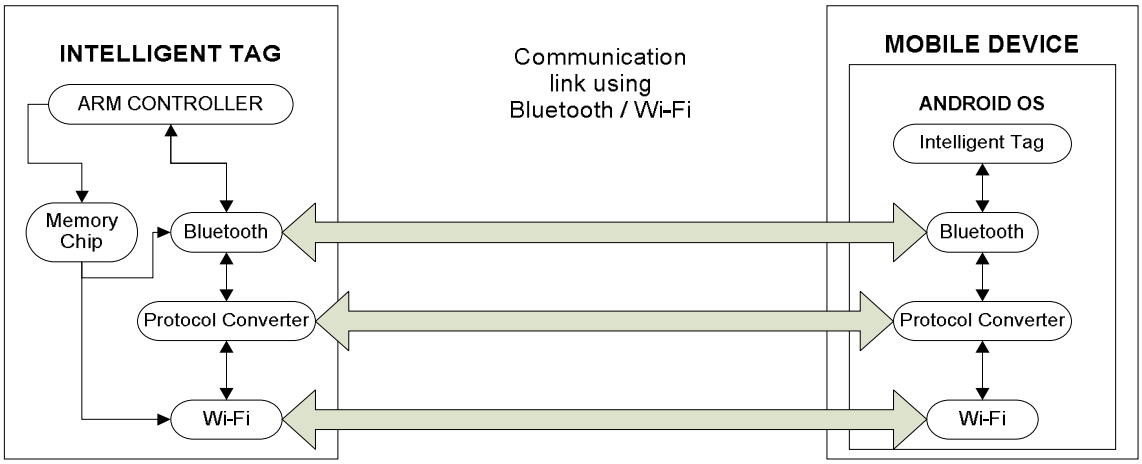

Figure 3 Communication Architecture of Intelligent Tag Management System

The main issue here in the aspect of Intelligent Tag Management System is providing enough intelligence such that the system will be able to detect the presence of any possible attack on the communication link between a Tag and the Mobile Device. This provision of intelligence to the system can be achieved by developing Intelligence Module along with Counter-measure Selector on both tag side and mobile device side. The functionality of Intelligence Module depicted in the Figure 4will be such that it senses whether there is any possibility of performing any attack on the communication link between a Tag and the Mobile Device. If the attack is confirmed then it passes the information about the type of attack to the Counter-measure Selector. The Counter-measure selector will implement counter attacking mechanism which is appropriate and relevant to the attack sensed. If the Intelligence Module senses that there is no possibility of attack on the communication link, then the Counter-measure Selector will be gone to idle state and the communication establishment will be done without any overhead of the counter attacking mechanism. The cloud is not used in this case. Direct communication between the mobile device and the Tag takes place using either the Bluetooth and mobile device which ever is selected on either side.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 2, Issue 6, June 2014

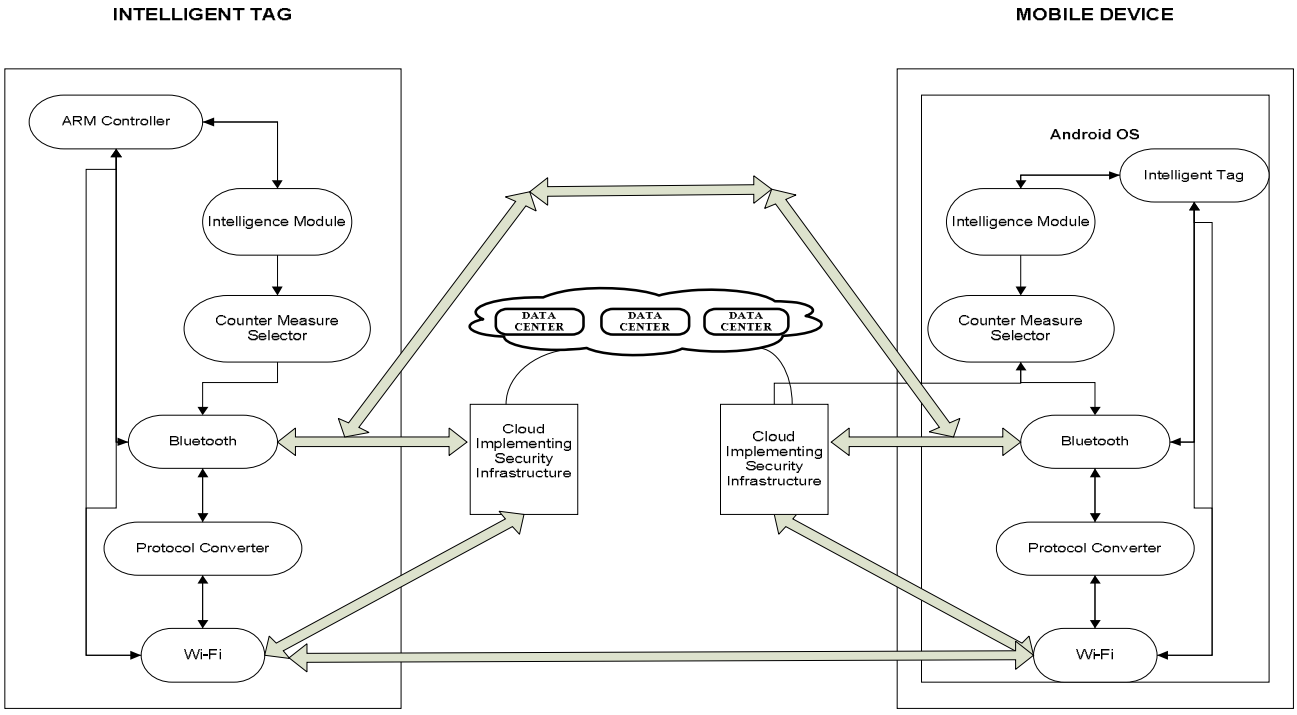

Figure 4.Effecting secured Communication between Tag and Mobile Device

The intelligence can be provided to the system by utilizing the Intelligence Module so that it can sense the possibility of any type of attack on the communication link and informs the Counter-measure Selector to implement appropriate counter attacking mechanisms. To perform this, the Intelligence Module is designed to sense the attacking based on certain parameters.

If the device on either side wants to send / receive data, then the intelligence module senses the frequency of access to critical data elements that govern the system. Frequency of accessing the critical data shall be recognized as an attack and automatically the requirement of authentication shall be implemented.

In the case of device attacking if the intruder tries for a handshake with variable number of frequencies the attack will be sensed and the counter measure of implementing RF signatures will be enforced. The device attacking sensor recognizes that an attack is taking place when frequency parameter is changing quite frequently while trying to establish the handshake.

When a man in the middle tries to attack after the hand shake between the peer team takes place, the transmission speeds varies drastically. The man in the middle is sensed while monitoring the transmission speeds and if the transmission speed varies and differ from the transmission speed established at the time of handshake, an attack is sensed and immediately the counter attacking mechanism like encryption and decryption shall be implemented in which case some of the low priority services shall be suspended. Several kinds of sensors are installed on the intelligent Tag side and a suitable counter attacking mechanism is initiated by the selector counter mechanism built into the Intelligent Tag. The mapping of the type of attack to a suitable counter attacking mechanism is shown in the Figure 5.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 2, Issue 6, June 2014

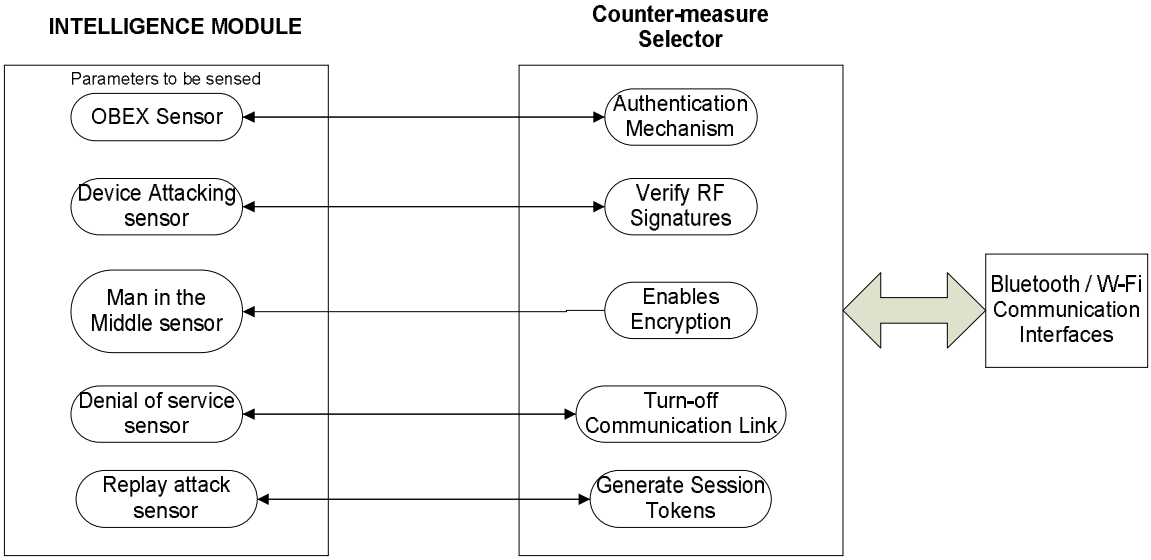

Figure 5.Parameters and Appropriate Counter Measures for Ensuring Security

When a communication link is established between two partners of the peer team, and one partner is transmitting messages of very high speed are when the same message is transmitted quite frequently, it will be sensed that an attack has been initiated, then a counter attacking mechanism is effected that terminates the communication Link.In the case replay attacks, sensing can be implemented by noticing the receipt of identical responses but with varying speeds in which case session tracking tokens will be implemented. The mechanism of session tracking will be enforced only when the repay attack is sensed.

V. EXPERIMENTING THE ATTACKING AND COUNTER ATTACKING

A software component has been installed on the TAG side to simulate the occurrence of a particular type of attack so that the software developed using the architecture proposed is tested thoroughly. Communication is effected through different combinations of communication protocols. The kind of attack that is affected is displayed on the Tag side LCD and Mobile side display system. Messages indicating the attack are sent from TAG side to mobile side. The messages are also displayed on the Tag side LCD and the mobile side display system.

The output displayed on the TAG and mobile side are tabulated and shown in the **Table I**. It could be seen from the table that under differentattacking conditions, the counter attacking mechanism imposed, the data sent from the Tag side and the data received on the mobile side. It could be seen from the table that the response time achieved is still within the limits even though more amount of code has to be executed due to implementation of counter attacking method.

The proposed method of security mechanism is implemented through Embedded-C under Integrated KEIL development tool kit. The Tag searches for the available devices within its vicinity. With the developed security mechanism, if there is no sign of attack on the communication link between a Tag and the mobile device, the system will perform the communication without any overhead of enabling the counter-measure mechanisms. If the system detects any attack being performed, then the appropriate counter-attacking mechanism is enabled and secures the communication link between them. This can be demonstrated by providing the experimental results as shown below.

VI.CONCLUSIONS

The devices used in the intelligent TAG systems are limited in the resources. The peer to peer communication between the TAG and the Mobile device is quite vulnerable. Adding the entire required infrastructure for securing the communication between the TAG and the mobile device requires many resources and providing such kind of resources is impracticable. Adding any software load for implementing the permanent counter attacking measures drastically effects the response time and throughput of transacting between the mobile device and the TAG. Intelligence has been

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 6, June 2014

added for sensing any attack and the counter attacking measure only come into force momentarily when any of the attacks are initiated. In-clouds are used for enforcing secured communication between the TAG and Mobile device.

REFERENCES

[1] Dieter Hutter, Günter Müller, Werner Stephan, and Markus Ullmann,Security and privacy aspects of low-cost radio frequency identification systems, Int. Conference on Security in Pervasive Computing" Springer Link - Lecture Notes in Computer. Science, Vol. 2802, Pg. 454-469, 2003

[2] Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita, Cryptographic approach to “privacy-friendly tags,”, RFID Privacy Workshop, MIT, MA, USA, 2003

[3] Dirk Henrici and Paul Müller, Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers, Int. Workshop on Pervasive Computing and Communication Security – PerSec, Pg. 149-153, 2004

[4] TassosDimitriou, 2005, A lightweight RFID protocol to protect against traceability and cloning attacks, International Conference on Security and Privacy for Emerging Areas in Communication Networks, IEEE, Pg. 59-66

[5] Young Ju Hwang, Su-Mi Lee, Dong Hoon Lee, and Jong In Lim Lim, 2005, Efficient authentication for low-cost RFID systems, Int. Conference. on Computational Science and its Applications - ICCSA,

[6] David Molnar and David Wagner, Privacy and security in library RFID: Issues, practices, and architectures, International Conference on Computer, Communication and Security – ACM CCS, Washington, DC, USA, Pg. 210-219, 2004

[7] Xingxin (Grace) Gao, Zhe (Alex) Xiang, Hao Wang, Jun Shen, Jian Huang, and Song Song, 2005, An approach to security and privacy of RFID system for supply chain, International Conference on E-Commerce Technology for Dynamic E-Business – CEC-East’04, Beijing, China, Pg. 164-168, 2005

[8] Dominic Spill and Andrea Bittau, Blue Sniff: Eve meets Alice and Bluetooth, University College London, 2006

[9] JKR Sastry, N. Venkatram, Y. Pavan Kumar, N. Rajesh Babu, On building intelligence for securing communication between the Tags and the Mobile Devices, International Journal Of Mobile and Adhoc Network - IFRSA, Vol. 3, Iss. 3, Pg. 297-302, 2012-13

[10] JKR Sastry, N. Venkatram, Y. Pavan Kumar, N. Rajesh Babu,Development of Software Architecture for Building Intelligence to Secure the Communication between the Tags and Mobile Devices, International Journal of VLSI and Embedded Systems-IJVES, Vol. 3, Iss. 2, Pg. 125-13, 2012-14

[11] JKRSastry, K Subba Rao, LSS Reddy, K Samuel Babu, J SasiBhanu, Attacking Embedded Systems through EMA, 2nd International conference on RF and signal processing, Pg, 627-631, 2010-1

[12] JKRSastry, K Subba Rao, N Venkataram J SasiBhanu,Attacking Embedded Systems through Power Analysis, Int. J. Advanced Networking and Applications, Vol. 2, Iss. 5, Pg. 811-816, 2011-1

[13] JKR Sastry, K Subba Rao, J Sasi Bhanu, Counter Attacking Electromagnetic attacks for securing Embedded Systems, International Journal of Advances in Science and Technology, Vol. 5, Iss. 1, Pg. 63-68, 2012-19

[14] JKR Sastry, K Subba Rao, J Sasi Bhanu, Counter Attacking method for Embedded Systems against Power Analysis, International Journal of Computer Information Systems, Vol. 5, Iss. 1, Pg. 17-23, 2012-20

[15] JKR Sastry, K Subba Rao, J Sasi Bhanu, "Counter attacking the timing attacks on Embedded Systems, International Journal of Advances in Science and Technology, Vol. 5, Iss. 1, Pg. 70-73, , 2012-21

[16] JKR Sastry, K Subba Rao, J Sasi Bhanu, 2012-22, "Counter attacking Fault Injections into Embedded Systems", International Journal of Research and Reviews in Applicable Mathematics & Computer Science, Vol. 2, Iss. 5, Pg. 63-69

[17] JKRSastry,C Ravi Shnaker, M Snigdha, MdSadiq, G Ashok, P Ravi Teja, , An efficient architecture for Enforcing Mobile security through In-Clouds, International Journal of Research and Reviews in Applicable Mathematics & Computer Science, Vol. 2, Iss. 2, Pg. 30-36, 2012-23

[18] JKR Sastry, K Subba Rao, J Sasi Bhanu, Attacking Embedded Systems through Fault Injection, 978-1-4244-9581-8/11/$26.00 © 2011 IEEE, 2011-2

[19] JKRSastry, K Subba Rao, J SasiBhanu, CH Jyotshna, Attacking Embedded systems through Timing Analysis, CSI Communication - October 2009, Pg. 37-40, 2009-1

[20] JKR Sastry, G. Bharathi, D. Srinivas,An efficient Architecture for the development of open cloud computing backbone, international Journal of computer Information systems, Vol.4, No. 2 Page 82-88, 2012

[21] Hanunah Othman,PE-TLBS: Secure Location Based Services Environment with Emphasis on Direct Anonymous Attestation Protocol, International Journal Multimedia and Image Processing (IJMIP), Vol. 1, Iss. 1, Pg. 40-52, 2011-1

[22] Sameer Hasan Al-Bakri,Securing peer-to-peer mobile communications using public key cryptography: New security strategy", International Journal of the Physical Sciences, Vol. 6, Iss. 4, Pg. 930-938, 2011-1

[23] SeifedineKadry, Design of Secure Mobile Communication using Fingerprint, European Journal of Scientific Research, Vol. 30, Iss. 30, Pg. 138-145, , 2009-1

[24] Dijiang Huang, MobiCloud: Building Secure Cloud Framework for Mobile Computing and Communication, Service Oriented System Engineering Fifth IEEE International Symposium, Pg. 27-34, 2010-1

[25] Hoang T Dinh,, A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches, Wiley Online Library, Pg. 1-38, 2011-1

[26] Satish Narayana Srirama, Secure Communication and Access Control for Mobile Web Service Provisioning, e-Centre for Informatics, Pg. 68-75, 2006-1

[27] AnandRaghunathan, Securing Mobile Appliances: New Challenges for the System Designer, Design, Automation and Test in Europe Conference and Exhibition Pg. 176-181, 2003-1

[28] JKR Sastry, G. Bharathi, D. Srinivas, An efficient Architecture for the development of open cloud computing backbone, International Journal of computer Information systems" Vol. 4 Iss. 2, Pg. 82-88, 2012

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Vol. 2, Issue 6, June 2014

Table 1 Experimental Result for Counter Attacking Methods

S.No	Attack Initiated	Counter Attack Initiated	Port Selected on the Tag side		Message sent from Tag side	Transmission		Port Selected on the Mobile side		Message Received on the Mobile Side	Reception		
			Wi-Fi	Bluetooth		Date	Time of Transmission	Wi-Fi	Bluetooth		Date	Time	Response in secs
1	-	-	√		POWS	10/06	10.00		√	POWS	10/06	10.01	0.01
2	Blue Snarfing attack	Authentication using PINs or Passwords		√	BSAT	10/06	10.05	√		BSAT	10/06	10.07	0.02
3	Blue Bugging attack	RF Signatures	√		BBAT	10/06	10.10	√		BBAT	10/06	10.12	0.02
4	Man-in-the-Middle attack	Encryption / Decryption with Time-out Mechanism		√	MMAT	10/06	10.20	√		MMAT	10/06	10.22	0.02
5	Denial of Service attack	Intrusion Detection System	√		DSAT	10/06	10.25	√		DSAT	10/06	10.27	0.02
6	Evil Twin Access Point attack	Avoid SSID broadcasting		√	ACAT	10/06	10.30		√	ACAT	10/06	10.32	0.02
7	Replay attack	Assignment of Session Tokens		√	RAAT	10/06	10.35	√		RAAT	10/06	10.37	0.02