Innovative Systems Design and Engineering
ISSN 2222-1727 (Paper) ISSN 2222-2871 (Online)
Vol.5, No.10, 2014
www.iiste.org

Enhancement of Security in RFID using RSA Algorithm

Jonathan Sangoro* Professor Waweru Mwangi Dr. Michael Kimwele
School of Computing and Information Technology
Jomo Kenyatta University of Agriculture and Technology, P.O. Box 62000 – 00200 Nairobi, Kenya
Lead author's mail; jonasangoro@gmail.com

Abstract
A huge revolution has occurred in Radio Frequency Identification (RFID) technologies during the past decades. More vendors are involved, and have invested in this technology, which promises wholesale changes across a broad spectrum of business activities. Currently, RFID systems are usually available in low, high, ultra-high, and microwave frequencies with passive, semi-passive (or semi-active) and active transponders or tags. Tags might be either Chipless, or contain a microchip with read only, or read and write memory. The component controlling communication in a RFID system is called a reader or interrogator, which can be stationary or portable depending on the application. In order for the tags to transmit their data, the tags must be in the reader's field or interrogation zone, and receive the necessary energy (in form of radio waves) from the reader. Although promising, RFID is not without its challenges, which arise from both a technological and usage point of View (IT Pro, 2005). A common concern with RFID is data security. Data Security is a key area in RFID usage, it determines wholly whether this technology will be adopted fully especially in this part of the world (Eastern and Central Africa) for business processes and automation. For this technology to be utilized fully and realized then the users of the system MUST be assured of their data's security.People who use devices that carry personal financial information, such as credit card or other ID numbers, do not want others to access their accounts. These are significant security vulnerabilities in RFID. Some researchers have proposed schemes that would require tags to authenticate readers, thus transmitting information only to authorized readers.This research paper addresses the security challenge in RFID by proposing RSA algorithm as a viable solution to encrypt data over transmission and also authenticate the reader and the tags.
Keywords: RFID, Security, authenticate, Data Security.

1.0 Introduction

RFID technology takes many forms, used in smartcards, implants for pets, passports, library books, and more. RFID is a rapidly growing technology that has the potential to make great economic impacts on many industries. While RFID is a relatively old technology, more recent advancements in chip manufacturing technology are making RFID practical for new applications and settings, particularly consumer item level tagging. These advancements have the potential to revolutionize supply-chain management, inventory control, and logistics etc.
At its most basic, RFID systems consist of small transponders or tags, attached to physical objects. When wirelessly interrogated by RFID transceivers or readers, tags respond with some identifying information that may be associated with arbitrary data records. Thus, RFID systems are one type of automatic identification system.

There are many kinds of RFID systems used in different applications and settings. These systems have different power sources, operating frequencies, and functionalities. The properties and regulatory restrictions of a particular RFID system will determine its manufacturing costs, physical specifications, and performance. Some of the most familiar RFID applications are item-level tagging with **Electronic Product Codes (EPC),** proximity cards for physical access control, and contact-less payment systems.

An EPC is a replacement for a barcode that can carry a larger amount of information and is electronically readable over distances up to 10 m, even when it is not visible.(A. Tanenbaum, 2011).
EPC Global was formed in 2003 to commercialize the RFID technology developed by the Auto-ID Center.
Widespread deployment has been hampered by the difficulty of competing with cheap printed barcodes, but new uses, such as in drivers licenses, are now growing.

1.1 RFID Applications

RFID applications are fueling a quiet business revolution that promises to speed up business process systems and change our lives. RFID is, in fact, already pervasive in our lives, Used to track everything from pets to prisoners to products.

1.2 RFID in Retail Sales/ Supply Chain Management

Globally, RIFD is being used for a number of commercial applications, and in particular for grocery and retail stores. The companies most interested in RFID have been drawn to it by the great potential for supply chain management. RFID technology holds the promise of substantial improvements in retail store logistics.

1.2.1 RFID in casino chips

Hecht (2003) reports that casinos will put RFID tags into their chips. The chips were launched later in 2004 and

allowed casino operators to spot counterfeits and thefts, and also to monitor the behaviour of gamblers. Counterfeit chips have long been a problem for casinos, and houses routinely mark their chips with inks visible only in infrared or ultraviolet light.
The tags could also help casinos manage large-scale theft. If a large stash of chips goes missing, casinos have to change their entire stock. This is unpopular with gamblers, since any chips that they have not cashed become worthless.

1.2.2 RFID in courier services

Booth-Thomas (2003) describes that the RFID usage has been implemented to track the shipments worldwide by different Courier Services like DHL, Fedex Express. In Singapore and Helsinki DHL tested it in anticipation of tracking the 160 million packages it ships annually. DHL Worldwide Express, has since gone global with RFID tracking.

1.2.3 RFID in automobile industry

By the virtue of RFID, Automated vehicle Identification System has shown remarkable and significant results. People are able to track automobiles of personal use or in logistics.
Booth-Thomas (2003) also tells us that traces of RFID use in automobiles goes back to1993. Taxes Instruments working with the Ford Motor Company, came up with a key that literally talks to a car. Use the wrong key, and the car is immobilized.

2.0 Rivest Shamir Aldeman (RSA) Encryption Algorithm

2.1 Introduction

This algorithm is based on the difficulty of factorizing large numbers that have 2 and only 2 factors (Prime numbers). The system works on a public and private key system. The public key is made available to everyone. With this key a user can encrypt data but cannot decrypt it, the only person who can decrypt it is the one who possesses the private key. It is theoretically possible but extremely difficult to generate the private key from the public key. This makes the RSA algorithm a very popular choice in data encryption.

2.2 RSA encryption algorithm Process

First of all, two large distinct prime numbers p and q must be generated. The product of these, we call n is a component of the public key. It must be large enough such that the numbers p and q cannot be extracted from it. It's 512 bits at least i.e. numbers greater than 10^{154}. We then generate the encryption key e which must be co-prime to the number $m = \varphi(n) = (p - 1)(q - 1)$. We then create the decryption key d such that $de \bmod m = 1$. We now have both the public and private keys.

Encryption

We let $y = E(x)$ be the encryption function where x is an integer and y is the encrypted form of x
$y = x^e \bmod n$

Decryption

We let $X = D(y)$ be the decryption function where y is an encrypted integer and X is the decrypted form of y
$X = y^d \bmod n$

2.3 Simple Example

1. We start by selecting primes $p = 3$ and $q = 11$.
2. $n = p\,q = 33$

$m = (p - 1)(q - 1) = (2)(10) = 20$.

3. Try $e = 3$

$gcd(3; 20) = 1$

$\Rightarrow e$ is co-prime to n

4. Find d such that $1 \equiv de \bmod m$

$\Rightarrow 1 = Km + de$

Using the extended Euclid Algorithm we see that $1 = -1(20) + 7(3)$

$\Rightarrow d = 7$

5. Now let's say that we want to encrypt the number $x = 9$:

We use the Encryption function $y = x^e \bmod n$

$y = 9^3 \bmod 33$

$y = 729 \bmod 33 \equiv 3$

$\Rightarrow y = 3$

6. To decrypt y we use the function $X = y^d \bmod n$

$X = 3^7 \bmod 33$

$X = 2187 \bmod 33 \equiv 9$

$\Rightarrow X = 9 = x$
$\Rightarrow$ It Works!

2.4 Implementing RSA Algorithm in RFID Applications

In this proposal we intend to implement RSA algorithm inside the software application in the reader. We choose to implement RSA in the reader since the reader is more technologically advanced than the tags and hence more robust which makes it easier for it to handle the complexity of the software more easily. In addition encrypting the software application in the reader is best since the tag has a very small memory in its integrated circuit and cannot reliably store a large software application in addition to the RSA algorithm required for security.

2.4.1 Encryption over the Air Interface

Encryption over the air interface requires both, the tag and the reader, to implement a cryptographic processor. Data is sent plainly to reader and there is where it is encrypted by RSA algorithm. Then the data is sent over the air interface to the tag which decrypts the data and stores it in its memory. If data is sent from the tag to the reader, the data are encrypted in the tag, and sent to the reader where they are decrypted again. The reader can than forward the data plainly or encrypt them again to the network for transport.

In this procedure the selection of the session key is taken care of by the reader or the application once both entities have been authenticated. During transfer the session key is encrypted with the authentication key. From then on the session key is used to encrypt data over the air interface. Readers as well as tags have to implement an asymmetric cipher, supporting encryption as well as decryption. RSA allows for some components used in the encryption to be reused by the decryption process.

This will ensure that data cannot be intercepted while in transit and if it is, the hacker will only obtain the ciphertext. Since the agenda of the hacker for interception of data was to obtain the plaintext most of the hackers will give-up at this point since they don't have the private key to decrypt the ciphertext back to plaintext. This is because the ciphertext will not hold any value to the hacker and so he cannot modify it or alter it for his own personal gain or malicious intentions.

But if the hacker wants to decrypt the ciphertext still, with no private key, the strength of the RSA algorithm comes in to play. This is because RSA algorithm is based on the difficulty of factorizing large numbers that have 2 and only 2 factors (Prime numbers). It is theoretically possible but extremely difficult to generate the private key from the public key. This makes the RSA algorithm a very popular choice in data encryption.

Also since RSA algorithm is a public key encryption it imposes a high computational burden, and tends to be much slower, thus the hacker may take years to crack the ciphertext.

The diagrams below are used to further elaborate on encryption over the air interface above. To accomplish this we must model a potential attacker. We differentiate between two basic types of attack. Attacker 1 behaves passively and tries to eavesdrop on the transmission to discover confidential information for wrongful purposes. Attacker 2, on the other hand, behaves actively to manipulate the transmitted data and alter it to his benefit.

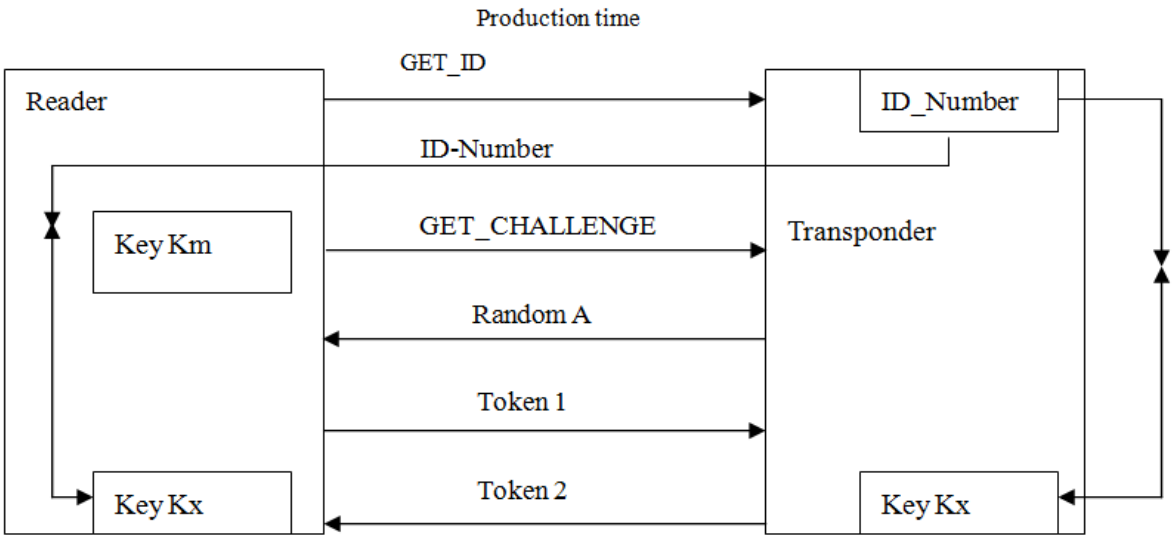

Figure 1: In an authentication procedure based upon derived keys, a key unique to the transponder is first calculated in the reader from the serial number (ID number) of the transponder. This key must then be used for authentication.

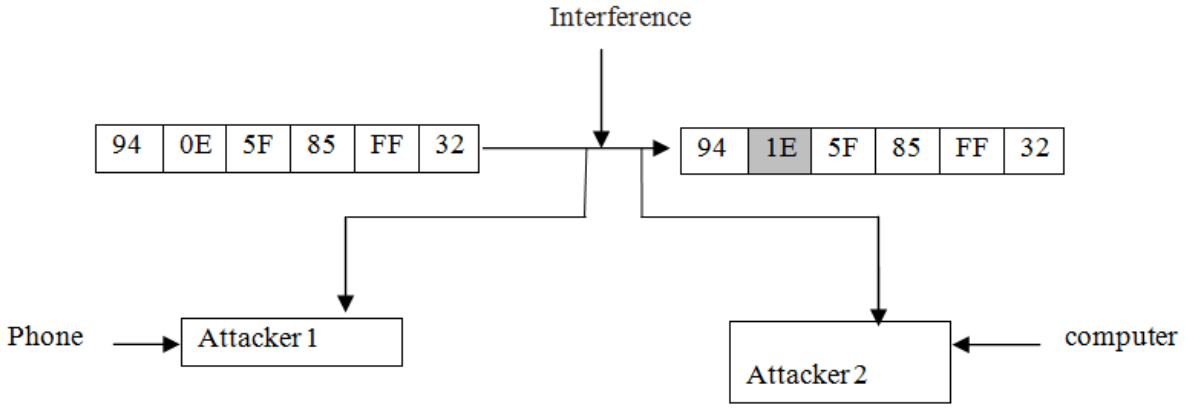

Figure 2: Attempted attacks on a data transmission. Attacker 1 attempts to eavesdrop, whereas attacker 2 maliciously alters the data

The cipher data is transformed back to its original form in the receiver using the secret key k' and RSA algorithm. The RSA algorithm is used to secure and protect data against both passive and active attacks. To achieve this, the plain text is encrypted prior to transmission so that a potential attacker can no longer draw conclusions about plain text.
Encrypted data transmission always takes place according to the same pattern.

The transmission plain text is transformed into cipher text using a secret *key* k and the RSA algorithm. Without knowing the encryption (RSA) algorithm and the secret key k a potential attacker is unable to interpret the recorded data. Thus it is not possible to recreate the plaintext from the cipher text.

If the keys k for ciphering and k' for deciphering are identical ($k = k'$) or in a direct relationship to each other, the procedure is a *symmetrical key procedure*. If knowledge of the key k is irrelevant to the deciphering process, the procedure is an *asymmetrical key procedure*.

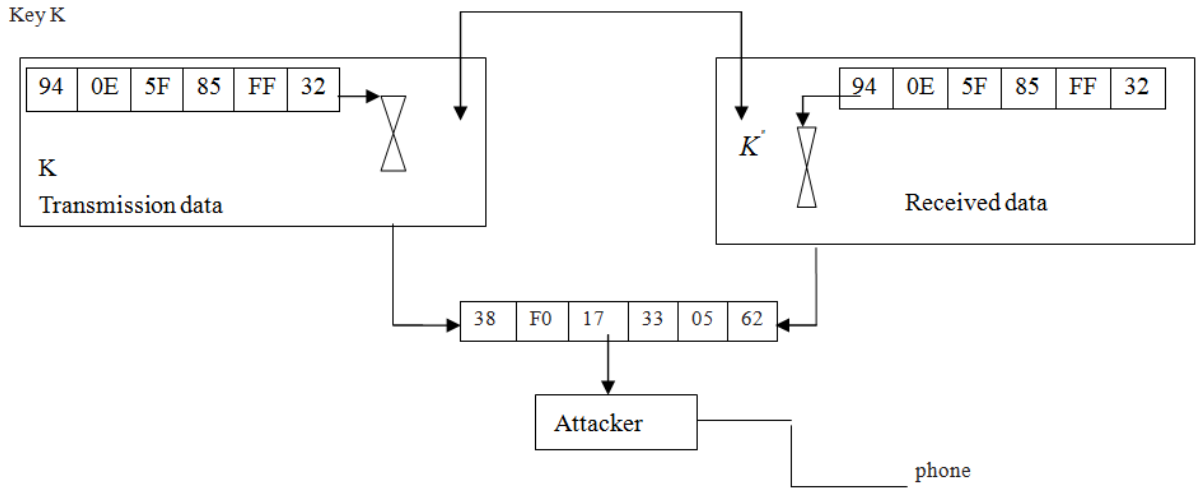

Figure 3: Encrypted data to be transmitted; this data can be effectively protected from eavesdropping or modification

From the above figures it is clear that RSA algorithms can improve the security of RFID systems which for a long time has had security flaws. The main advantage is that even if an attacker intercepts data when in transmission, he will only acquire the ciphertext from which it is highly unlikely to decipher the plaintext.

The reason for the difficulty is deciphering the ciphertext is that RSA algorithm deals with factoring two prime numbers. These two prime numbers are usually very big integers and may take a very long time to be

broken down so as to acquire the private key k' which will be used to decipher the ciphertext.

2.5 Test Data

This research paper is going to use the following example to encrypt a password using a public key and RSA algorithm, then later decrypt the ciphertext using a private key.

If the resultant decrypted data matches the original plaintext that was encrypted then we would have proven beyond doubt that our theory for using RSA algorithm to enhance data security in RFID applications is sound.

Example

Let U = 5 and V = 11. This gives R a value of 55, and:

Phi (55) = (5 - 1) * (11 - 1) = 4 * 10 = 40.

Now, we need to find numbers to fit the equation:

P * Q = 1 (mod 40).

Let P=7

7 * Q = 1 (mod 40).

What would that make Q? If we rewrite this equation to get rid of the unfamiliar modulus arithmetic, we have:

7 * Q = K * 40 + 1, where K can be any number.

The first value for Q that works is 23:

7 * 23 = 161 = 4 * 40 + 1.

So we have 7 for P, our public key, and 23 for Q, our private key.

To make our cipher work, you may recall that the values we use for T must be less than R, and also relatively prime to R. We also don't want to use 1 for T, because 1 raised to any power whatsoever is going to remain 1.

2	3	4	6	7	8	9	12	13	14	16	17	1
A	B	C	D	E	F	G	H	I	J	K	L	M
19	21	23	24	26	27	28	29	31	32	34	36	37
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
38	39	41	42	43	46	47	48	49	51	52	53	
Sp	0	1	2	3	4	5	6	7	8	9	*	

Table 1. Conversion table

The password we will encrypt is "VENIO"

V	E	N	I	O
31	7	19	13	21

Table 2. Conversion table

To encode it, we simply need to raise each number to the power of P modulo R.

V: 31^7 (mod 55) = 27512614111 (mod 55) = 26

E: 7^7 (mod 55) = 823543 (mod 55) = 28

N: 19^7 (mod 55) = 893871739 (mod 55) = 24

I: 13^7 (mod 55) = 62748517 (mod 55) = 7

O: 21^7 (mod 55) = 1801088541 (mod 55) = 21

So, our encrypted message is 26, 28, 24, 7, 21 -- or "RTQEO" in our personalized character set.

When the message "RTQEO" arrives on the other end of our insecure phone line, we can decrypt it simply by repeating the process -- this time using Q, our private key, in place of P.

R: 26^23 (mod 55) = 350257144982200575261531309080576 (mod 55) = 31

T: 28^23 (mod 55) = 19259043800372760688541191131627 52 (mod 55) = 7

Q: 24^23 (mod 55) = 55572324035428505185378394701824 (mod 55) = 19

E: 7^23 (mod 55) = 2736874734008091634 3 (mod 55) = 13

O: 21^23 (mod 55) = 25765808751082182919290758696 61 (mod 55) = 21

The result is 31, 7, 19, 13, 21 -- or "VENIO", our original message.
Thus it works!!!!

3.0 Conclusion

When using RFID to transmit and decode data there are three important security scenarios to consider. First, where RFID is implemented to improve an existing business process, it can automate activities and thereby reduce the potential business and security risks caused by human error. Second, RFID itself can induce new risks to a process; mostly unlike barcodes, RFID tags will be used in security-sensitive applications such as ticketing, access control and product authentication. Therefore security is needed to keep automated aspects and invisible properties under control, and prevent any risk of the process becoming susceptible to abuse. Owing to the high level of automation that RFID provides, a security incident could cause great harm before countermeasures will be effective since RFID readers can read any tags in close proximity with or without authentication. Third, as RFID is a data gathering and process measurement technology, it can completely enable new business applications. Activities and actions unable to previously be accurately measured can now deliver effective metrics. Again, security plays a major role delivering the accountability required to engender trust in the data and activities provided by these applications.

The three reasons above all regard to security, this simply implies that security is of utmost importance when dealing with RFID technologies. This is because RFID tags have a problem, they always (when no user input is required to initiate communication) respond to queries by readers without their owners' knowledge or consent. This makes achieving security more challenging.

Thus it is for this purpose that this research paper proposes RSA algorithm as the encryption algorithm to enhance security when transmitting data between the reader and the tags. RSA algorithm is a public key encryption that factors two prime numbers to generate a public key and private key to encrypt plaintext and decrypt the ciphertext respectively.

The reason why this paper focuses on RSA algorithm is that even an attacker intercepts the data while in transmission, he will need to have the private key to decipher the ciphertext back to plaintext. Though possible to decrypt the ciphertext without the private key, an attacker is going to have a hard time trying to decipher the ciphertext since RSA algorithm uses two co-prime numbers which are big integers. Thus it will be a time consuming and tedious process to decrypt the ciphertext.

RFID is the future of technology in Africa and for companies and businesses to invest deeply into it, they must be assured of their data's security, which will help them avoid litigations due to data leakage while at the same time enabling them to maximize their profits through automation processes which will enable them realize their Return on Investment.

4.0 References

A.Juels and R. Pappu, (2003), "Squealing euros: Privacy protection in RFID-enabled banknotes", In proceedings of Financial Cryptography – FC'03, LNCS, volume 2742, Springer-Verlag, pages 103-121.
A.Tanenbaum, D. Wetherall "Computer Networks"2011.
AES page available via http://www.nist.gov/CryptoToolkit
Artz, Matthew (2003). City library adopts controversial RFID chips. Retrieved October 10, 2003, from http://www.berkeleydaily.org/article.cfm?issue=10-10-3&storyID=17547
Auto-ID Center, (2002), "860MHz-960MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical communication Interface Specification Proposed Recommendation Version 1.0.0", Technical Report MIT-AUTOID-TR-007, November.
Booth-Thomas, Cathy (2003, October 20). The see-it-all chips. *Time,* 162 (15), 12-17
Chachra, Vinod (2003). Experiences in implementing RFID solutions in a multi-vendor environment. *IFLA Conference, Berlin, August, 2003.* Retrieved August 15, 2003, from http://www.ifla.org/IV/ifla69/paper/132e-chachra.pdf
Cooper, R.B. and Zmud, R.W. (1990), "Information technology implementation research: a technological diffusion approach", *Management Science*, Vol. 36 No.2, pp. 123-139.
Denyer, D., Tranfield, D. and van Aken, J.E. (2008), "Developing design propositions through research synthesis", *Organization Studies*, Vol. 29 No. 3, pp. 393-413.
EPC global US, http://www.epcglobalus.org, 2006, last accessed on February 6, 2006.
Diffie, W., Hellman, M.: New directions in cryptography. IEEE Transactions on Information Theory 22(6), 644–654 (1976)
EPC Radio-Frequency Identity Protocols Generation 2 Identity Tag (Class 1):Protocol for Communications at 860 MHz-960 MHz. EPC Global Hardware Action Group (HAG), EPC Identity Tag (Class 1) Generation 2,

Last-call Working Draft Version 1.0.2, 2003-11-24.
FIPS 180-2. Secure Hash Standard, http://csrc.nist.gov/publications/, 2002
Gershenfeld, N., and Krikorian, R., and Cohen, D.: ‘‘The Internet of Things,’’*Scientific American*, vol. 291, pp. 76–81, Oct. 2004.
Gregor, S. and Jones, D. (2007), “The anatomy of a design theory”, *Journal of the Association for Information Systems*, Vol. 8 No. 5, pp. 312-335.
H. Aljifri, and N. Tyrewalla, (2004), “Security model for Intra-Domain Mobility Management Protocol”, *Int. J. of Mobile Communications*, Vol. 2, No.2, pp. 157 – 170.
Hecht, Jeff (2004). Casino chips to carry RFID tags. *New Scientist*. Retrieved September 02, 2004, from http://www.newscientist.com/news/news.jsp?id=ns99994542
Holmström, J., Ketokivi, K., Hameri, A.-P. (2009b), “Bridging Practice and Theory: A Design Science Approach”, *Decision Sciences*, Vol. 40 No. 1, pp. 65-87.
Juels, A., Weis, S.A. (2005). Authenticating Pervasive Devices with Human Protocols.
Advances in Cryptology – Crypto ’05. Lecture Notes in Computer Science. Volume 3621. Pages 293-308.
W. Küchlin, “Public key encryption,” ACM SIGSAM Bulletin, August 1987, pp. 69-73.
Mezrich, Ben (2002). Hacking Las Vegas. *Wired Magazine, 10(09)*. Retrieved September 02,
2004, from http://www.wired.com/wired/archive/10.09/vegas.html
RFID Journal. (2003). Gillette Confirms RFID Purchase. RFID Journal. Available at:
http://www.rfidjournal.com/article/articleview/258/1/1/. (Last Accessed: March 11, 2006.)
R.Fishkin and B. Jiang “Some Methods for Privacy in RFID Communication,”, *Intel Research*; http:// www.intelresearch.net/Publications/Seattle/062420041517_243.pdf
Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM, 21(2):120–126, 1978.
S.Weiss, “RFID Privacy Workshop:Concerns, Consensus, and Questions,” *IEEE Security & Privacy*,Mar.-Apr. 2004.
Sample, A., Yeager, D., Powledge, P., Mamishev, A., and Smith, J.: ‘‘Design of an RFID- Based Battery-Free Programmable Sensing Platform,’’ *IEEE Trans. On Instrumentation and Measurement*, vol. 57, pp. 2608–2615, Nov. 2008.
Simon, H.A. (1997), *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organizations*, *4th edition*, The Free Press, NewYork, NY.
Van Aken, J.E. and Romme, G. (2009), “Reinventing the future: adding design science to the repertoire of organization and management studies”, *Organization Management Journal*, Vol. 6 No. 1, pp. 5-12.
Van Dorp, K.-J. (2001), “Tracking and tracing: A structure for development and contemporary practices”, *Logistics Information Management*, Vol. 15 No. 1/2, pp. 24-33.
Visich, J.K., Li, S., Khumawala, B.M. and Reyes, P.M. (2009), “Empirical evidence of RFID impacts on supply chain performance”, *International Journal of Operations & Production Management*, Vol. 29 No. 12, pp. 1290-1315.
Welbourne, E., Battle, L., Cole, G., Gould, K., Rector, K., Raymer, S.,Balazinska, M., and Borriello, G.: ‘‘Building the Internet of Things Using RFID,’’ *IEEE Internet Computing*, vol. 13, pp. 48–55, May 2009.
Yin, R.K. (1994), *Case Study Research: Design and Methods. 2nd edition*, Sage Publications, CA, USA.
Yin, R., 2002. Case Study Research: Design and Methods. *SAGE Publications, Edition. 3.*

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar