INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue4)

Available online at: www.Ijariit.com

A Hybrid Approach for Enhancing Security in RFID Networks

Bhawna Sharma[#1], Dr. RK Chauhan[#2]

Student[#1], Professor[#2]

Department Of Computer Science and Engineering

DCSA, Kurukshetra Haryana

Abstract- RFID (Radio-Frequency Identification) is a technology for automatic identification of things and people. Human beings are skillful at identifying things under many different challenge circumstances. A bleary-eyed person can quickly pick a cup out of coffee on a cluttered breakfast dining table each day, as an example. Computer sight, though, executes jobs which are such. RFID might be considered an easy method of explicitly objects that are labeling facilitate their "perception" by processing devices. An RFID device frequently only called an RFID label is a microchip that is small for wireless information transmission. It is generally mounted on an antenna in a package that resembles an adhesive sticker that is ordinary. The word "RFID" to denote any RF device whose function that is main identification of an object or person. This definition excludes simple products like retail stock tags, which simply indicate their particular presence and on/off condition during the standard end of the practical range. It also excludes products being transportable smart phones, which do a lot more than merely identify by themselves or their particular bearers. Numerous cryptographic models of security neglect to show crucial features of RFID systems. A straightforward design that is cryptographic as an example catches the top-layer communication protocol between a tag and audience. In the reduced layers are anti-collision protocols along with other RF that is basic notably enumerate the safety dilemmas present at multiple interaction layers in RFID methods. This work proposes a hybrid that is brand new and AES based Encryption mechanism for RFID program.

I. INTRODUCTION

RFID (Radio-Frequency Identification) is a technology for automated recognition of objects and individuals. Humans are skillful at distinguishing objects under a variety of challenge circumstances. A bleary-eyed individual can easily pick a cup away from coffee on a cluttered breakfast table into the morning, for instance. Computer vision, though, performs tasks that are such. RFID might be seen as a means of explicitly objects that are labeling facilitate their "perception" by computing devices.

An RFID device – frequently just called an RFIDtag–isa microchip that is small for wireless data transmission. It is generally attached to an antenna in a package that resembles an adhesive sticker that is ordinary. The microchip itself is often as small as a grain of sand, some 0.4mm2. An RFID tag transmits data over the fresh atmosphere in reaction to interrogation by an RFID reader.

Both in the press that is popular academic circles; RFID has seen a swirl of attention in the past few years. One reason that is very important this is actually the work of large organizations, such as Wal-Mart, Procter and Gamble, and the United States Department of Defense, to deploy RFID as a tool for automatic oversight of their supply chains. Thanks to a mixture of dropping tag costs and RFID that is vigorous standardization we're on the brink of an explosion in RFID use.

Advocates of RFID see it as a successor to your optical barcode familiarly printed on consumer services and products, with two benefits that are distinct:

1. **Unique identification:** The sort is recommended by a barcode of item on which it really is imprinted, e.g., "This is a club this is certainly 100g of brand 70% chocolate." An RFID label goes a step further. It emits a volume this is certainly special is serial differentiates among many millions of identically manufactured things; it might suggest, e.g., that "This is 100g bar of ABC brand 70% chocolate, serial no. 897348738." 1 The unique identifiers in RFID tags can work as tips to a database entry offer that is containing is wealthy for singular items.
2. **Automation:** Barcodes, being optically scanned, need line-of-sight contact with visitors, and positioning that is therefore careful is physical of items. Except in probably the most rigorously controlled environments, barcode scanning requires intervention that is specific. In contrast, RFID tags are readable without line-of-sight contact and without accurate placement. RFID readers can scan tags at prices of hundreds per second. Today as an example, an RFID reader by a warehouse dock door cans scan stacks of passing crates with high accuracy. In the near future that is near point-of-sale terminals could possibly be able to scan all of things in moving shopping carts.

Due to tag cost and a hodgepodge of logistical complications – like the ubiquity of steel shelving, which interferes with RFID scanning – RFID tags are unlikely appearing regularly on consumer items for some years. Retailers have expressed interest, though, in ultimately tagging items that are individual. Such tagging would, for instance, address the problem that is perennial of depletion on retail shelves that is high priced in terms of lost sales.

Today, RFID is fruition that is seeing the tagging of crates and pallets, that is, discrete bulk amounts of products. RFID tagging improves the timeliness and accuracy of information regarding the movement of goods in supply chains.

Today the problems of clandestine RFID tracking and are that is inventorying of concern, since RFID infrastructure is scarce and fragmentary. As explained above, the tagging of individual items which are retail probably some years away. Once RFID becomes pervasive, nevertheless, as is almost inevitable, the privacy problem will assume more dimensions that are solid. One harbinger of the RFID that is emerging infrastructure Verisign's EPC Discovery Service. It creates a view that is unified of of individual EPC tags across businesses.

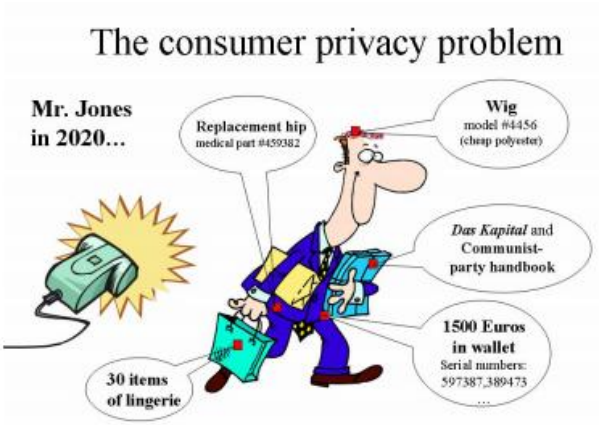

Fig. 1. An illustration of potential consumer privacy problems of RFID

RFID privacy is already of concern in several areas of everyday life:

- **Toll-payment transponders:** Automated toll-payment transponders small plaques positioned in windshield corners are commonplace all over the world. A court subpoenaed the data collected from such a transponder for use in a divorce case, undercutting the alibi of the defendant in at least one celebrated example.
- **Euro banknotes:** As early as 2001, the media reported plans by the European Central Bank to embed RFID tags in banknotes as an measure that is anti-counterfeiting. This task seems increasingly implausible provided the attendant technical problems (and of course the target that is purported of 2005). It has served don and doff, however, as a flashpoint for privacy concerns.
- **Libraries:** Some libraries have implemented RFID systems to facilitate book check-out and inventory control and to reduce stress that is repeated in librarians. Issues about monitoring of guide selections, stimulated in part by the USA Patriot Act, have fueled privacy concerns around RFID.
- **Passports:** an organization that is worldwide due to the fact International Civil Aviation Organization (ICAO) has promulgated directions for RFID-enabled passports along with other travel documents. America has mandated the use among these standards

by twenty-seven "Visa Waiver" countries as a condition of entry for their citizens. The mandate has seen delays because of its challenges being technical changes in its technical parameters, partly in a reaction to lobbying by privacy advocates.

II. RFID ATTACK MODELS

In order to define the notions of "secure" and "private" for RFID tags in a manner that is rigorous we should first ask: "Secure" and "private" against what? The clear answer that is best is a formal model that characterizes the capabilities of potential adversaries. In cryptography, such a model typically takes the form of an "experiment," a program that intermediates communications between a model adversary, characterized as a algorithm that is probabilistic or Turing machine), and a model runtime environment containing system components (often called oracles). The adversary would have admission to system components representing tags and readers within the model for an RFID system, for example.

The adversary is thought to have more-or-less unfettered access to system components within the runtime environment in many cryptographic models. This will make feeling: An adversary can more or less access any networked computing device at any moment in security models for cyberspace. A server, for example, is always on-line, and responds freely to queries from around the planet. For RFID systems, however, around the-clock access by adversaries to tags is usually too strong an assumption. An adversary should have physical proximity to it a sporadic event in most environments in order to scan a tag. It is important to adapt RFID security models to realities that are such. Because low-cost RFID tags cannot execute standard cryptographic functions, they cannot offer security that is meaningful models which can be too strong.

III. SECURING RFID TAGS

A tag's standard that is underlying act as a quick, distinguishing bit of information. AO also note potential risks during the physical and manufacturers will plump for the tag that is five-cent. They will address privacy and security concerns utilizing other, cheaper measures. (The barebones safety features of the EPC Class-1 Gen-2 standard reinforce this point.) Having less cryptography in basic RFID is a impediment that is big security design; cryptography, all things considered, is one regarding the lynchpins of data security.

1)Privacy protecting Schemes

Most schemes which are privacy-protecting basic tags have focused on the consumer privacy problems discussed above. (Industrial privacy, i.e., information secrecy, is important too, but less frequently considered.) We now enumerate the various approaches which can be proposed the customer privacy problem.

1. **"Killing" and "Sleeping":** EPC tags address consumer privacy with a straightforward and provision that is draconian Tag "killing." When a"kill is received by an EPC tag" command from a reader, it renders itself permanently inoperative. This kill command is PIN protected to prevent wanton deactivation of tags. A reader also needs to transmit a tag-specific PIN (32 bits very long in the EPC Class-1 Gen-2 standard) to kill a tag. As "dead tags tell no tales," killing is a privacy measure that is impressive. It is envisioned that once RFID tags become prevalent on retail items, point-of-sale devices will destroy the RFID tags on purchased items to protect consumer privacy. As an example, after you roll your supermarket cart through an automated checkout kiosk and pay the resulting total, each of the RFID that is associated is killed in the spot.

Removable RFID tags help a approach that is similar. Marks and Spencer, for example, include RFID tags on garments in their shops. These RFID tags, nevertheless, live in price tags, and are therefore easily discarded and removed.

Killing or tags that are discarding customer privacy effectively, but it eliminates every one of the post-purchase benefits of RFID for the consumer. The receipt less item returns, smart devices, aids for the elderly, and other beneficial systems described early in the day in this specific article will maybe not make use of deactivated tags. And perhaps, such as libraries and rental shops, RFID tags cannot be killed they track because they must survive over the lifetime associated with objects. For these reasons, it's crucial to look beyond killing for more approaches that are balanced consumer privacy.

2. **The renaming approach:** Even when the identifier emitted by an RFID tag has no meaning that is intrinsic it can still enable tracking. For this good explanation, merely encrypting a tag identifier does not solve the issue of privacy. An encrypted identifier is it self just a meta-identifier. It is static, and therefore subject to monitoring like any other number that is serial.

2) Universal re-encryption:

The JP system relies on a solitary, universal pair that is keySK, P K). A general RFID system would likely require multiple key pairs while just one key pair might suffice for a unified monetary system. Straightforward extension of JP to multiple pairs that are fundamental $(SK_1,PK_1),(SK_2,PK_2),...(SK_n,PK_n)$, however, would undermine system privacy. however, would undermine system privacy. To re-encrypt a ciphertext C,it would be necessary to know under which public key PK_i it is encrypted, information that is potentially privacy-sensitive.

3. **The proxying approach:** Rather than depending on public RFID readers to enforce privacy protection, consumers might carry their own instead privacy-enforcing devices for RFID. As already noted, some phones that are mobile RFID functionality. They might ultimately support privacy protection. Researchers have proposed systems that are several these lines:
4. **Distance measurement:** The barebones resources of basic RFID tags urge exploration of privacy schemes that shy away from expensive, high-level protocols and instead exploit lower protocol layers. The ratio that is signal-to-noise of audience signal in an RFID system provides a rough metric associated with distance between a reader and a tag. They postulate that with some additional, low-cost circuitry a tag might attain rough dimension of the distance of an reader that is interrogating. FRJ propose that this distance serve as a metric for trust. A tag might, for example, launch information that is general"I amattached to a bottle of water") when scanned at a distance, but release more specific information, like its unique identifier, only at close range.
5. **Blocking:** A scheme that is privacy-protecting they call blocking. Their scheme varies according to the incorporation into tags of a little that is modifiable a privacy bit. A '0' privacy bit marks a tag as susceptible to unrestricted scanning that is public a '1' bit marks a tag as "private." JRS refer to the room of identifiers with leading bits that are'1 a privacy zone. A blocker tag is a RFID that is unique that prevents unwanted scanning of tags mapped into the privacy zone.

3) Authentication Schemes

We now have discussed the ways in which fundamental RFID tags can combat counterfeiting by offering supply-chain visibility that is enhanced. As we have actually noted, nevertheless, outside a host of truly information that is seamless counterfeiting of RFID tags can facilitate counterfeiting of consumer goods. Yet authentication that works well of RFID tags the type we consider let me reveal very hard.

Juels shows a straightforward method to repurpose the kill function in EPC tags to achieve restricted resistance that is counterfeiting. Normally, the kill PIN authenticates a reader to a tag in order to authorize the deactivation of the tag. Alternatively, this verification can be reversed, and the kill PIN can serve to authenticate instead the tag to the reader. The protocol that is basic in co-opts the ability of tags to distinguish between valid and spurious kill PINs.

IV. SYMMETRIC-KEY TAGS

Let us now turn our focus on the course of RFID tags with richer safety capabilities, those capable of computing symmetric-key (cryptographic one-way) functions.

For brevity, we use loose notation in this section, and assume extremely familiarity that is basic cryptographic primitives. Recall that a hash that is cryptographic h has the special property that for a random bit sequence M of sufficient size, it's infeasible to compute M from understanding of the hashed value h(M) alone. Hashing involves no secret key (and it is consequently only loosely called a symmetric-key function). On the other hand, symmetric-key encryption, sometimes called secret key encryption, relies upon a key k that is secret. A message or plaintext M are encrypted as a ciphertext with this particular key $C=e_k$ [M]. Only with knowledge of k is it feasible to decrypt C and recovers M.

(a) Cloning

In principle, symmetric-key cryptography can go far toward eliminating the problem of tag cloning. With a simple challenge-response protocol like the following, a tag Ti can authenticate itself to a reader with which it shares the keyk_i:

1) The tag identifies itself by transmitting the valueT_i.
2) The reader generates a random bitstringR(often called anonce) and transmits it to the tag.
3) The tag computes$H=h(k_i,R)$, and transmits H.
4) The reader verifies that$H=h(k_i,R)$.

Alternatively, and more or less equivalently, the tag can return e_{ki} [R]. (Note that for the moment here, we set aside privacy considerations, and suppose that tags identify themselves.)

Provided that the hash function h(or encryption function e) is well constructed and appropriately deployed, it is infeasible for an attacker to simulate T_i successfully without physically attacking the tag.

In practice, however, resource constraints in commercial RFID tags sometimes lead to the deployment of weak cryptographic primitives, and thus vulnerable authentication protocols, as our discussion now illustrates.

1. **The Digital Signature Transponder (DST):** Texas Instruments (TI) manufactures a low-frequency, cryptographically enabled RFID device called a Digital Signature Transponder (DST). The DST serves as a theft-deterrent in millions of automobiles – many Ford that is late-model and automobiles, for instance. Present as a tiny, concealed chip in the ignition key of the driver, the DST authenticates the key to a reader near the key slot as a precondition for beginning the engine. (The metal portion of the

ignition key in isolation will not start the vehicle.) The DST can be present in SpeedPass™ payment that is wireless, utilized by an incredible number of customers mainly at ExxonMobil petrol stations in North America.

The DST executes a challenge-response that is simple essentially like that described above. It includes a keyki that is secret. The DST executes an encryption function eand outputs in a reaction to a random challenge R from a reader $C=e_{k_i}$ [R]. The challengeRis 40 bits in length, the response Cis 24 bits in length. Of particular note is the length of the secret key k_i. It is only 40 bits. As cryptographers know, this is quite short by today's standards: A key of this length is vulnerable to brute-force attack that is computational. Perhaps acknowledging the key-length that is insufficient of DST, Texas Instruments hasn't published details of the encryption algorithm e, rather preferring the approach of "security through obscurity."

I. **Reverse-engineering:** The researchers determined the unpublished encryption algorithm e in the DST. They relied on three things:

A TI DST reader, available in an evaluation kit;

Some blank DSTs, meaning tokens with programmable secret keys; and

A loose schematic of the encryption algorithm e published on the Internet by a scientist at TI. With the reader and blank tags, the researchers were able to determine the output valuee_k [R]for any key k and challenge R. Based on the published schematic, they carefully formulated and tested sequences of key/challenge pairs to derive operational details of the encryption algorithm e. They did not physically probe the DST in any way.

II. **Key cracking:** Having determinede, the researchers implemented a hardware "cracker" costing several thousand dollars. This cracker consisted of an array of 16 FPGA boards. Given two input-output pairs(R_1,C_1) and (R_2,C_2) skimmed from a target DST, it proved capable of recovering a secret key in about thirty minutes on average. The cracker operated by brute force, meaning that it searched the full space of2 40 possible DST keys.

III. **Simulation:** The researchers constructed a programmable radio device that exactly simulates the output of any target DST.

The JHU-RSa team demonstrated their assault in the field. Simulating the DST present in an ignition key (and using a copy of the metal portion), they "stole" their very own automobile. They also purchased gasoline at a service section using a clone of their SpeedPass™ that is own token!

2. **Reverse-engineering and side channels:** Most RFID tags are and could continue to be too inexpensive to include tamper resistance mechanisms. Physically invasive attacks are mainly of concern for RFID tags that serve as authenticators, and of concern that is greatest when such assaults leave no physical traces or let the construction of perfect physical replicas of target devices. For example, a reverse-engineered RFID-based payment device might be cloned to effect fraudulent payments (on-line controls serving as an important but limited countermeasure). Reverse-engineering of smartcards is an increasingly well studied area; even hardened devices have yielded to probing that is successful modest resources.

V. RELATED WORK

Junichiro Saito, Jae-CheolRyou et. al. (2004) [1] In this paper, a Radio-Frequency-Identification (RFID) tag is a small and cheap device which is combined in IC chip and an antenna for radio communications. It emits an ID in response to a query from a radio communication device called as a reader. For this reason, the RFID tag is used for management of goods and it is used as a substitute for a bar code. However, RFID system may infringe on a consumer's privacy because it has a strong tracing ability. Although ID of a RFID tag can be encrypted, it is possible to pursue an object by tracing specific information. Therefore, they discuss the privacy protection using universal re-encryption proposed. Since the system does not protect a modification of the information on RFID tags, it can be exploited by an attacker. Therefore they point out two attacks using modification of the information on RFID tags. Moreover, they offer two proposed schemes for addressing the problem.

Martin, Feldhofer, Sandra Dominikus et. al. (2004) [2] In this paper, radio frequency identification (RFID) is an emerging technology which brings enormous productivity benefits in applications where objects have to be identified automatically. This paper presents issues concerning security and privacy of RFID systems which are heavily discussed in public. In contrast to the RFID community, which claims that cryptographic components are too costly for RFID tags, they describe a solution using strong symmetric authentication which is suitable for today's requirements regarding low power consumption and low die-size. We introduce an authentication protocol which serves as a proof of concept for authenticating an RFID tag to a reader device using the Advanced Encryption Standard (AES) as cryptographic primitive. The main part of this work is a novel approach of an AES hardware

implementation which encrypts a 128-bit block of data within 1000 clock cycles and has a power consumption below 9 µA on a 0.35 µm CMOS process.

Miyako, Ohkubo, Koutarou Suzuki et. al. (2005) [3] In this paper, in the future ubiquitous-computing environment, RFID tags will be attached to all kinds of products and other physical objects, even to people, and could become a fundamental technology for ubiquitous services where the tags are used to identify things and people automatically. However, despite this promise, the possible abuse (or just excessive use) by retailers and government agencies of RFID's tracking capability raises questions about potential violations of personal privacy. Here, they discuss two protest campaigns—one against apparel manufacturer Benetton in Italy, the other against Tesco in the U.K.—that reflect the growing concern among consumer-privacy advocates regarding how RFID might affect personal data. Consumers against Supermarket Privacy Invasion and Numbering (CASPIAN, www. nocards.org) criticized Benetton's plans to attach tags to its products, leading to a boycott of those products. Earlier this year, CASPIAN similarly criticized Tesco for conducting experimental trials of tags on a variety of its products.

Jeremy Landt et. al. (2005) [4] In this paper, radio frequency identification (RFID) is an integral part of our life, which increases productivity and convenience. It is the term coined for short-range radio technology used to communicate mainly digital information between a stationary location and a movable object or between movable objects. This RFID system uses the principle of modulated backscatter where it can transfer the data from the tag to the reader. The tag generally reads its internal memory of stored data and changes the loading on the tag antenna in a coded manner corresponding to the stored data. RFID is a technology, which spans systems engineering, software development, encryption etc., and thus there are many engineers involved in the development and application of RFID and at present the shortage of technical and business people trained in RFID is hampering the growth of the industry.

Giuseppe Ateniese, Jan Camenisch et. al. (2005) [5] In this paper, We introduce a new cryptographic primitive, called insubvertible encryption, that produces ciphertexts which can be randomized without the need of any key material. Unlike plain universal re-encryption schemes, insubvertible encryption prevents against adversarial exploitation of hidden channels, by including certificates proving that the ciphertext can only be decrypted by authorized parties. The scheme can be applied to RFID tags, providing strong protection against tracing. This enables post-sale applications of manufacturer-issued RFID tags while preserving the privacy of consumers. The functionality required of the RFID tags is minimal, namely that they be re-writable (many-writable). No cryptographic capabilities are required of the tags themselves, as the readers perform all necessary computations.

Ari Juels et. al. (2006) [6] In this paper surveys recent technical research on the problems of privacy and security for radio frequency identification (RFID). RFID tags are small, wireless devices that help identify objects and people. Thanks to dropping cost, they are likely to proliferate into the billions in the next several years—and eventually into the trillions. RFID tags track objects in supply chains, and are working their way into the pockets, belongings, and even the bodies of consumers. This survey examines approaches proposed by scientists for privacy protection and integrity assurance in RFID systems, and treats the social and technical context of their work. While geared toward the nonspecialist, the survey may also serve as a reference for specialist readers.

Pedro Peris-Lopez et. al. (2006) [7] In this paper, low-cost Radio Frequency Identification (RFID) tags affixed to consumer items as smart labels are emerging as one of the most pervasive computing technology in history. This can have huge security implications. The present article surveys the most important technical security challenges of RFID systems. We first provide a brief summary of the most relevant standards related to this technology. Next, they present an overview about the state of the art on RFID security, addressing both the functional aspects and the security risks and threats associated to its use. Finally, they analyze the main security solutions proposed until date.

VI. OVERVIEW OF RSA CRYPTOSYSTEM

In RSA, the plaintext and the cipher text are thought to be integers between 0 and n-1, where n is the modulus. The size that is typical of is 1024 bits. Nevertheless, the size that is advised of is 2048 bits as 640 bits key is no more secure by now. The RSA algorithm is composed of three sub algorithms that are described below:

(a) Key Generation Algorithm

The key set is generated by using the following algorithm:

1. Select two large prime numbers p and q (e.g. 1024 bits each) such that $p \neq q$.

2. Compute modulus n = p.q
3. Calculate totient, φ(n) = (p-1). (q-1)
4. Choose an integer (public exponent) e, 1 ¡ e ¡φ(n), such that gcd(e, φ(n)) = 1.
5. Compute the secret exponent d, 1 ¡ d ¡φ(n), such that *d.e*≡ 1 (mod n).

The public key is (n,e) And the private key is (n, d).

(b) Encryption

Encryption is done by using the following steps:-

1. Obtain the recipient's public key (n, e).
2. Represent the plaintext message as a positive integer m.
3. Compute the cipher text c = m^e mod n.
4. Send the cipher text c to receiver.

(c) Decryption

Message is decrypted by using the following steps:-

1. Receiver uses his own private key (n, d) to compute m = c^d mod n.

Extracts the plaintext from the integer representative m

VII. COMPUTATIONAL ISSUES OF RSA

1. Selecting the primes p and q:
   In the first step, a random number of —n—/2 bit-length for p is selected. Then the lowest bit and two highest bits are set to ensure p is odd and the highest bit of n will be set. Finally, Miller-Rabin algorithm is applied to ensure that p is a prime number. Prime number q is determined following the same steps.
2. Choosing the value of e:
   The mathematical requirement gcd(e, φ(n)) = 1 is equivalent to the
   gcd(e, p-1) = q and
   gcd(e, q-1) = 1 that can be satisfied by choosing a prime number for e. However, for fast modular exponentiation operation, e is chosen among 3, 17 and 65537 as only two bits are set for these three values.
3. Calculating the value of d:
   The requirement *d.e*≡1 (mod φ(n)) is equivalent to d = d^{-1} (mod φ(n)) which is determined by Extended Euclidean Algorithm.
4. Modular Exponentiation for Encryption and Decryption:
   - For encryption: c = m^e mod n can be efficiently computed by selecting an appropriate value for e such as {3; 17 or 65537}.
   - for decryption: Decryption operation can be efficiently completed by using Chinese Remainder Theorem (CRT) in the following manner:
     c^dmod n = ($v_p x_p$ + $v_q x_q$) mod n
     where, v_p = c^d mod p, v_q = c_d mod q
     and x_p = q (q^{-1} mod p), x_q = p (p^{-1} mod q)
   - Further efficiency can be obtained by applying Fermat's Little Theorem to calculate $v_p$and v

   v_p = c^d mod p
   = $c^{(u(p-1)+v)}$ mod p
   = $(c^{(p-1)})^u c^v$mod p
   = $(1)^u c^v$ mod p
   = c^v mod p

   As (v ¡ d), required computation is less than the previous one.
5. Modular exponentiation algorithm:
   Modular exponentiation is the fundamental computation step of RSA that can be effectively performed by using the following formula:

A^B mod n = $\left(\prod b^i \neq 0[A^{2^i} mod\ n]\right) mod\ n$

VIII. LIMITATIONS OF THE RANDOM WAYPOINT MODEL AND OTHER RANDOM MODELS

The Random Waypoint model and its variants are made to mimic the movement of mobile nodes in a manner that is simplified. Because of its simpleness of analysis and implementation, they are widely accepted. However, they may not acceptably capture specific mobility characteristics of some realistic situations, including temporal dependency, spatial dependency and restriction that is geographic:

1. **Temporal Dependency of Velocity:** The velocity of mobile node is a memory less random process, i.e., the velocity at current epoch is independent of the last epoch in Random Waypoint and other random models. Therefore, some mobility that is extreme, such as sudden end, unexpected acceleration and sharp turn, may frequently occur in the trace generated by the Random Waypoint model.
2. **Spatial Dependency of Velocity:** The mobile node is regarded as an entity that moves independently of other nodes in Random Waypoint and other random models. This sort of mobility model is categorized as entity mobility model.
3. **Geographic Restrictions of Movement:** The mobile nodes can move freely within simulation field without any limitations in Random Waypoint and other random models. However, in many realistic cases, especially for the applications used in urban areas, the movement of a node that is mobile be bounded by hurdles, buildings, streets or freeways.

IX. SIMULATION PARAMETERS

Following table describes the simulation parameters for RFID mobility in MATLAB, each node properties is defined in MATLAB Structure.

Parameter	Value
Node POSITION_X_INTERVAL	10-30
Node POSITION_Y_INTERVAL	10-30
Node SPEED_INTERVAL	0.2-2.2
Node PAUSE_INTERVAL	0-1
Node WALK_INTERVAL	2.00-6.00
Node DIRECTION_INTERVAL	-180-180
SIMULATION_TIME	500
Number of Nodes	20
Public Key Encryption	RSA
Private Key Encryption	AES

Node POSITION_X_INTERVAL: X position of the Node at any given moment, updates due to Random Way Point Model
Node POSITION_Y_INTERVAL: Y position of the Node at any given moment, updates due to Random Way Point Model
Node SPEED_INTERVAL: Speed Range of Each Node factor of 0.2 to 2.2x speed with respect to stationary nodes.
Node PAUSE_INTERVAL: For how long a node will stay stationary
Node WALK_INTERVAL: For how long a node will stay moving
Node DIRECTION_INTERVAL: In which direction the node will be moving.
SIMULATION_TIME: Overall Simulation Time of the Node.
Number of Nodes: Total number of nodes present in the Simulation (default: 20)
Public Key Encryption: Encryption Scheme used to Encrypt Messages using Public Key of the node and Decryption using the Private keys.
Private Key Encryption: Encryption Scheme used to Encrypt Private key of the Node using the Location of each node before Sending any data.

Steps of the Algorithm

Step 1: Receiver **R** Requests data from the node **S**, only receiver knows the exact location of itself.
Step 2: On receiving request from the **R** node the sender initiate public key Exchange using RSA algorithm and stores keys P_k as Private key of the node R and P_u as the public key to encrypt the data.

Step 3: Node S then Request the Location L_{Rxy} of the node R.
Step 4: After receiving request from the node S the R sends its location L_{Rxy} to the node S.
Step 5: S then Encrypts the private key of the by using L_{Rxy} as Private key using AES algorithm
Step 6: for multiple recipients the Same process in repeated and a matrix is formed in following manner and forwarded to recipients.

Encrypted Data (RSA)	L_{Rxy}private key of the receiver 1 (AES)
	L_{Rxy}private key of the receiver 2 (AES)
	….
	L_{Rxy}private key of the receiver N (AES)

Step 7: After receiving the packet the recipient decrypts the private key using its location and then decrypts the data sent by the sender.

X. CONCLUSION AND FUTURE WORK

Many concepts and protocols, given by different authors, have been proposed in this report which will help in securing an Internet of Things (RFID) network. Introduction of the dynamic cipher that is adjustable certificate protocol is given. This protocol uses matrices that are key. In this protocol we take advantage of key matrices and shop key that is same at all of the interacting nodes. Thus when text that is ordinary encrypted to cipher text at the giving part, the sender transmits the cipher text without the key that is to be used to decrypt the message. In spite, the transmitter delivers the co-ordinate of the matrix that is key one of the keys is kept.
For little devices, resource limitations make it challenging to individually secure all layers. Securing only the application layer renders the network ready to accept assaults, while safety focused only at the network and link layer might introduce inter-application that is feasible threats. Thus, the limited sourced elements of things may require sharing of keying material and protection that is typical between levels. Such cross layer concepts should really be considered for an redesign that is RFID-driven of security protocols.

XI. REFERENCES

[1] Junichiro Saito, Jae-CheolRyou, and Kouichi Sakurai. "Enhancing privacy of universal re-encryption scheme for RFID tags." In Embedded and Ubiquitous Computing, pp. 879-890. Springer Berlin Heidelberg, 2004.
[2] Martin, Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer. "Strong authentication for RFID systems using the AES algorithm." In Cryptographic Hardware and Embedded Systems-CHES 2004, pp. 357-370. Springer Berlin Heidelberg, 2004.
[3] Miyako, Ohkubo, Koutarou Suzuki, and Shingo Kinoshita. "RFID privacy issues and technical challenges." Communications of the ACM 48, no. 9 (2005): 66-71.
[4] Jeremy Landt. "The history of RFID." Potentials, IEEE 24, no. 4 (2005): 8-11.
[5] GiuseppeAteniese, Jan Camenisch, and Breno de Medeiros. "Untraceable RFID tags via insubvertible encryption." In Proceedings of the 12th ACM conference on Computer and communications security, pp. 92-101. ACM, 2005.
[6] Ari Juels. "RFID security and privacy: A research survey." Selected Areas in Communications, IEEE Journal on 24, no. 2 (2006): 381-394.
[7] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda. "RFID systems: A survey on security threats and proposed solutions." In Personal wireless communications, pp. 159-170. Springer Berlin Heidelberg, 2006.

