IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 7, Issue 3, March 2018

Clone Detection Using Double-Track Approach For Rfid-Enabled Supply Chains

Dhumal T.A.[1], Jadhavar S.S.[2], Shinde A.S.[3], Navadkar N.K.[4], Shaikh T.U.[5], Sarwade P.L[6]

Assistant Professor, CSE Department, BIT Collage, India [1]

Student, CSE Department, BIT Collage, India[2,3,4,5,6]

Abstract: Toward enhancing the regular clone identification method whose execution might be influenced by powerful changes of supply chains and misread, we introduce a novel and successful clone location approach, named twofold track discovery, for radio recurrence identification-empowered supply chains. As a feature of a label's properties, verification data is built into labels with the goal that the arrangement of all verification data in the gathered label occasions frames a period arrangement succession. Real labels can be separated from clone labels because of the disparity in their verification groupings which are built as items own along the production network. The verification grouping together with the succession framed by business activities performed amid the supply chains yield two tracks which can be evaluated to recognize the nearness of clone labels. Hypothetical examination and trial comes about demonstrate that our proposed system is compelling, sensible, and has a moderately high clone discovery rate when contrasted and a main strategy around there.

Keyword: Clone detection, RFID, twofold track discovery, EPC.

I. INTRODUCTION

In radio frequency identification (RFID) enabled supply chains, every product is equipped with an RFID tag which contains a unique product identifier: electronic product code (EPC). Each supply chain participant stores some particular EPC information related to the event in its EPC Information Services (EPCIS) repository for processing. Supply chain partners can record, store, and share information related to these identifiers through RFID infrastructures (e.g., EPC global Network).While RFID technology allows logistics enterprises to implement a transparent and real-time supply chain management system and deliver significant improvements for ware-house management efficiency, it, unfortunately, also brings in some problems. For example, criminals and terrorists carrying clone tags would endanger the safety of patients in medical industry [1], clone tags impose a serious threat to military and national security [2], and the presence of cloned tags can cause severe economic losses in the logistics industries [3] [6], which directly affects consumers' interests and properties. To resolve these issues, clone-attack prevention and detection methods have been studied.

Prevention: Prevention techniques based on cryptography, such as encryption, decryption, and authentication, typically involve key distribution and management policies. These safety measures usually not only require extra storage spaces, but also need additional encryption operations [3], [7], and therefore are not suitable to be implemented in those low-cost tags that have weak computational power.

Detection: Since no form of prevention strategy can completely prevent clone attacks, clone attack detection techniques will thus be a beneficial supplement. In many cases, when the tracking system malfunctions, or a system security is compromised, counterfeiters may inject unlimited number of clone products into the supply chain. In this regard, clone detection techniques are the only means to protect consumer’s interests and constitute a fundamental component of a secure infrastructure. The study of RFID clone tags detection thus not only possesses certain strategic significance, but presents an interesting challenge for researchers as well.

In this paper, we propose an effective clone detecting approach: Double-Track Detection (DTD). Since events are generated by reading RFID tags, we store a verification sequence value in a tag memory; this verification sequence value is updated to C 1 after the tag is detected by the reader, and the related tag event data (updated) is stored in the local database. In order to protect privacy, the initial-value should be randomized. In cases when an attacker modifies the value of, our scheme can still detect clones because it may cause duplicated -values. We assume that tag EPC cannot be rewritten, but tag memory can be read and rewritten, and the -value is of 8 bits. With products owing in the supply chain, all values form a verification sequence which will show a certain kind of regularity with a series of trajectory. While the verification sequence constitutes one track of product information, business action information of

DOI 10.17148/IJARCCE.2018.7386

events forms another track. Our clone detection scheme works by checking the correctness of these two tracks with reference to specific tag events. Since it does not depend on a preened structure of supply chains or a product information own, it is exile regarding the dynamically changing supply chains, and suitable for general deployment.
The Section 2 reviews related work in RFID clone detection. Section 3 briefly describes RFID-enabled supply chains. Section 4 introduces our proposed clone detection approach, and is evaluated in Section 5 with comparison with other. Section 6 concludes the paper.

II. RELATED WORK

Stake, These, and Fleischer presented a primary study about the supply chain RFID security solutions that is based on track-and-trace, which highlights the negative impact of incomplete tracks on cloning attack detection when partners don't record or share track data. Lee and Bang proposed a pattern mining algorithm, using event track records to mine the legitimate supply chain model by which counterfeit product detection algorithms can be generated. Although these proposed mechanisms are all suitable for the low-cost (EPC C1G2) tags, they need the related supply chain structure and product of information in order to work properly, resulting in some weak performance and less robustness when faced with supply chain dynamic changes, product recalls and product transportation errors.

Zenith, Fell Mann, and Capcom proposed a track-and-trace-based privacy-preserving clone detection method, which detects clones by verifying the correctness of two consecutive events in time, without relying on the global knowledge of supply chain structures or the product on information. It works well with product recalls and product delivery errors. However, the clone detection rate is not improved. A pattern-matching approach was proposed in [16] by Kerschbaum and Orel to detect illegal transactions between supply chain partners. In Zanetti, Capcom, and Jules proposed to add a random tail and a tail pointer in each user-denied block in EPC tags. In each event, the reader increments the tail pointer and updates the pointed random bits. Clone products can be detected by inspecting the consistency between tails and tail pointers. Although enjoying a relatively high detection rate, this method seriously reduces the tag processing speed, and induces considerably large communication and memory overheads. Bu et al. [5] and Bu, Liu, and Xiao [7] suggested the use of hash functions in detecting clones. Under this scheme, two tags with the same ID always response to the reader queries simultaneously when they are within the reading range of the reader, resulting in the fact that genuine tags and clone tags will make inevitable irreconcilable collisions. Because it requires that genuine tags and clone tags be present at the same time and in the location, this method can only be used in certain scenarios.

III. RFID-ENABLED SUPPLY CHAIN AND EVENTS: A FORMAL VIEW

We consider RFID-enabled supply chains in which each product is equipped with an RFID tag; a product and its tag are considered to be inseparable. Every RFID tag contains a unique product identifier (EPC) which is to be read by different readers at different locations. Each tag-reading at a location creates an event which is stored in the local EPC Information Services (EPCIS) database that can be accessed and shared by supply chain partners via RFID infrastructures (e.g., EPC global network), so all the events related to a specific tag data are stored in a distributed manner. Supply chain participants can send related event information (for example, EPC C partner's database address) to Discovery Services (DS). Data stored in partners and DS databases can be accessed through authentication and access control mechanisms, and the DS creates a virtual product history path by accessing the distributed EPCIS repositories. Participants in supply chains include manufacturers, wholesalers and retailers, and we assume that the legitimate supply chain participants are not malicious (i.e., they will not cover up attackers).

An event corresponds to a reading of the RFID tag of a product. In local databases, an event for a product (identified by its id D EPC) that occurs at time t, denoted by e (id; t),is formally defined as follows: $e(id, t) = (`, \tau, \nu, \sigma) \in L \times T \times V \times S$
L = set of locations of supply chain participants
$T = \{rcv, shp, inv\}$
$V = \{0 \ldots 255\}$
$S = \{tru, fls\}$

where the attributes $` \in L$, $\tau \in T$, $\nu \in V$, and $\sigma \in S$ represent the location, a business transaction (receiving (rcv), shipping (shp), and inventory (inv)), the verification value, and the success (tru) or failure (fls) of updating the verification value in an event, respectively. Two special events e(id, tin) and e(id, tout) are created for a product when the product initially enters into the supply chain (i.e., when an EPC tag is assigned to a product at the manufacturer) and eventually leaves the supply chain (i.e., the product is sold at a retailer). So clone products can be easily detected using the corresponding events if they appear on the supply chain before e(id, tin) or after e(id, tout). An event is considered to be proprietary and confidential. Any supply chain participants only know their direct business partners, and can join or leave the supply chain at any time. We define clones as counterfeit products carrying legitimate EPCs, and multiple readings of one tag are assumed to be processed during the data collection stage.

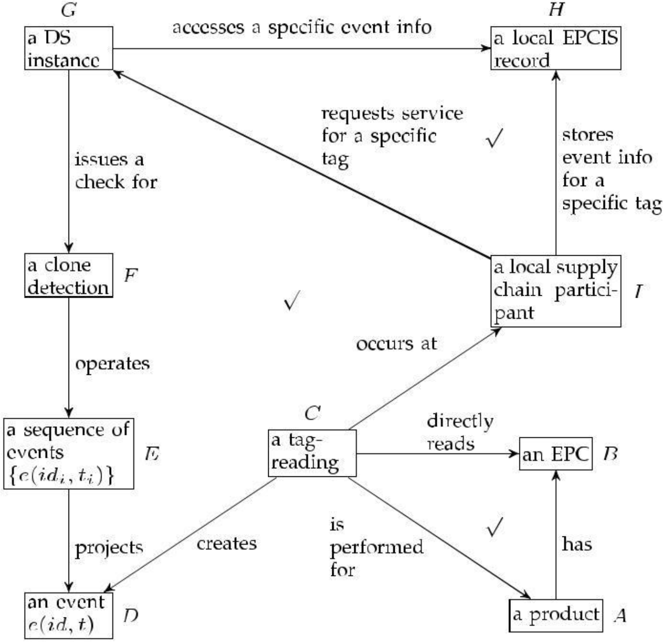


FIGURE 1. The Olog model for RFID-enabled supply chain activities.

The activities associated with clone detection in RFID-enabled supply chains can be understood and formalized as an Olog model [18] as shown in Fig. 1, in which each box represents a type and each arrow denotes a (mathematical) function from the source box to the target box. The check mark (√) indicates that the enclosing figure is commutative, i.e., any two paths leaving from the same source box and ending at the same target box are equivalent. For example, the check mark in the triangle ABC states that the EPC which is being read in a tag-reading is the same EPC of the product for which the tag-reading action is performed.

IV. CLONE DETECTION MECHANISM

A verification sequence is formed by following some stipulated rules except that the initial item in the verification sequence may be assigned randomly by the manufacturer. Our approach detects the presence of clones by examining, for two consecutive events in time, the successiveness of the values and the consistency of business transactions.

A. VERIFICATION SEQUENCE CONSTRUCTION

A verification sequence for a tag is built up by successively updating the ν-value in the tag. ν-value updating is completed in a non-interactive manner, i.e., by the participating RFID reader alone. It is a natural extension of the tag-reading process in the sense that a new event containing the updatedν-value will be created after the current event (containing an old ν-value) has been read. The procedure of the ν-value updating includes the following steps: (1) Read the EPC and the ν-value from the tag memory. (2) Increase ν by 1 and write the result back into the tag memory. Tag-writing mistakesare indicated by the status attribute σ. When the reader does not receive an acknowledging response from the tag for the writing operation, or the writing operation fails, σ will be set to fig. (3) Create an event e (id, t) = (`, τ, ν, σ), and add it to the local database. Of course, supply chain participants must agree to the above specifications. In addition, the reader is capable of signaling a request at any time to disable the σ-attribute.

B. EVENT COLLECTION

Any supply chain participants may request some product related information (e.g., EPC + partners database address) from the DS which then accesses the distributed EPCIS databases to create a history path of events for this product.

C.DOUBLE TRACK RULE VERIFICATION

All available events associated to a specific tag EPC are collected and ordered by time to form an event sequence. The machinery of our clone detection approach can be precisely expressed by the following formula and rules

$$e(id;\ t)D(`;\ ;\ ;) \qquad (1)$$

$$\frac{e(id;\ t_i)_2D\ rcv}{} \qquad (2)$$

DOI 10.17148/IJARCCE.2018.7386

$e\ (id;\ t_{iC1})_2 D\ shp{=}inv \qquad e(id;\ t_i)_1 D\ e(id;\ t_{iC1})_1$

$e(id;\ t_i)_2 D\ shp$

$e(id;\ t_{iC1})_2\ \ D\ rcv\ \ e(id;\ t_i)_1\ 6De(id;\ t_{iC1})_1$

$e(id;\ t_i)_2 D\ inv$

$e(id;\ t_{iC1})_2\ \ D\ inv{=}shp\ \ e(id;\ t_i)_1\ D\ e(id;\ t_{iC1})_1$

$e\ (id;\ t_i)_4 D\ tru\ D\ e(id;\ t_{iC1})_4$

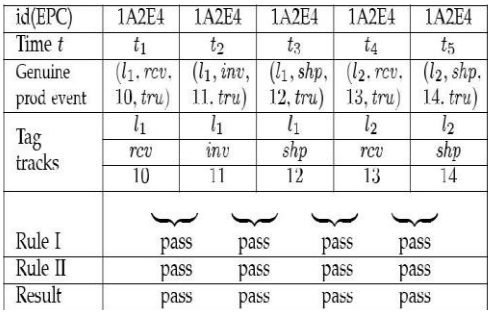
$e\ (id;\ t_{iC1})_3 \qquad e(id;\ t_i)_3\ \ 1\ \ (\text{mod } 256)$

Where ti and ti+1 represent two arbitrary consecutive points in time, and e (id, t)k (k = 1, 2, 3, 4) means the k-the component of e (id, t). Formula (1) is just a redisplay of the event formulated in Section 3. Rule (2) states that for any given event, if the business transaction of this event is ‘‘receiving’’ (e (id, ti)2 = rcv), then this event must be followed by a shipping or inventory event recorded at the same location. In a similar fashion, rule (3) stipulates that a shipping event recorded at a location must be followed by a receiving event recorded at a different location, and rule (4) states that an inventory event must befollowed by either an inventory or a shipping event at the same location. Rule (5) states that if the verification values of two time-consecutive events are well documented, then the verification value of the later event is one more than that of the early event modulo 256. We can regroup rules (2)-(5) into two (composite) rules as follows

Rule I = rule (2) ∨ rule (3) ∨ rule (4)
Rule II = rule (5)
and any pair of time-consecutive events passes the check if and only if both Rule I and Rule II are satisfied.

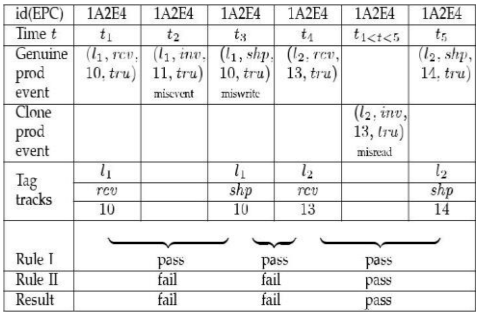
D. CLONE DETECTION

We can examine the correctness of all such pairs for any given set of events through the above two rules, thereby forming a double-track inspection for clones. If all examinations yield correct (pass) results, then there is no presence of clones; otherwise, there are some clones. These two situations are illustrated in Fig. 2(a) and 2(b) respectively, where 2(a) shows the detection result with no clone products and 2(b) with clone products. There are three types of accidents: misread, and miswrite and their respective effects are illustrated in (c). For instance, due to the misevent at time t2 or the miswrite at time t3 the first examination yields a ‘‘fail’’ and therefore causes a false alarm since there is no clone involved in that examination. The result of the third examination should be a ‘‘fail’’ since there is a clone product; but because of the misreading of the clone tag at time t4<i<5, no event is created for this clone product for that time and thus the existence of the clone is concealed. We now address the issue of determining the cause of failure when the double-track rule verification yields a negative result. That is, does the failure suggest the presence of?



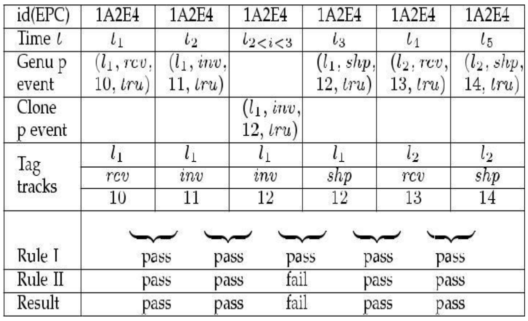
id(EPC)	1A2E4	1A2E4	1A2E4	1A2E4	1A2E4
Time t	t_1	t_2	t_3	t_4	t_5
Genuine prod event	$(l_1, rcv, 10, tru)$	$(l_1, inv, 11, tru)$	$(l_1, shp, 12, tru)$	$(l_2, rcv, 13, tru)$	$(l_2, shp, 14, tru)$
Tag tracks	l_1	l_1	l_1	l_2	l_2
	rcv	inv	shp	rcv	shp
	10	11	12	13	14
Rule I	pass	pass	pass	pass	
Rule II	pass	pass	pass	pass	
Result	pass	pass	pass	pass	

(a)



id(EPC)	1A2E4	1A2E4	1A2E4	1A2E4	1A2E4	1A2E4
Time t	t_1	t_2	t_3	t_4	$t_{1<t<5}$	t_5
Genuine prod event	$(l_1, rcv, 10, tru)$	$(l_1, inv, 11, tru)$ misevent	$(l_1, shp, 10, tru)$ miswrite	$(l_2, rcv, 13, tru)$		$(l_2, shp, 14, tru)$
Clone prod event					$(l_2, inv, 13, tru)$ misread	
Tag tracks	l_1		l_1	l_2		l_2
	rcv		shp	rcv		shp
	10		10	13		14
Rule I		pass		pass	pass	
Rule II		fail		fail	pass	
Result		fail		fail	pass	

(b)



id(EPC)	1A2E4	1A2E4	1A2E4	1A2E4	1A2E4	1A2E4
Time l	l_1	l_2	$l_{2<i<3}$	l_3	l_1	l_5
Genu p event	$(l_1, rcv, 10, lru)$	$(l_1, inv, 11, lru)$		$(l_1, shp, 12, lru)$	$(l_2, rcv, 13, lru)$	$(l_2, shp, 14, lru)$
Clone p event			$(l_1, inv, 12, lru)$			
Tag tracks	l_1	l_1	l_1	l_1	l_2	l_2
	rcv	inv	inv	shp	rcv	shp
	10	11	12	12	13	14
Rule I	pass	pass	pass	pass	pass	
Rule II	pass	pass	fail	pass	pass	
Result	pass	pass	fail	pass	pass	

(c)

DOI 10.17148/IJARCCE.2018.7386

FIGURE 2. Rule verification results for events generated (a) by a genuine product, (b) by both genuine and clone products together, and (c) by both genuine and clone products while misevent, misread, and miswrite are considered.
Some clone products or is it caused by the combination of misevent, misread, and miswrite? Assume P_{mr} is the misreading probability of the reader. The readings of the tags can be considered as binomially distributed as shown in formula (6), where N_m is the total number of missing events that would be required to restore all incorrect sequences in the considered track, and N is the total number of events. In order to investigate the relationship between failed rule verifications and the minimum number of possible missing events, we focus on Rule I and ``forget'' about Rule II and the business transaction inv since these two elements can only increase the number of possible missing events. The result is shown in Table 1 where $`_i$ and $_i$ are used to denote e (id; t_i) $_1$and e (id; t_i) $_2$respectively to save the space. Whenthe calculated probability exceeds a certain threshold, then the cause of the rule verification failure can be regarded as clones; otherwise, it is due to the combination of misevent.

V. PERFORMANCE EVALUATION

In this section, we are evaluating our clone detection scheme by a simulation. A 15-partner supply chain in the form of a 4-level binary tree is constructed by using the Arena [19] simulation software. Products flow in the supply chain from the manufacturer to retailers via one or several distributors. Our clone detection approach will be triggered when a genuine or counterfeit product leaves the supply chain (sold to customers). The manufacturer (top level) produces 1000 genuine products every day, and 10 clone products are randomly injected into different levels in the supply chain on a daily basis.1 Special c parameters of the simulation are shown in Table 2 (adapted from [17]).attributes of each event is extended by ν and σ, resulting in only 7% increases in event size

A. STORAGE SPACE REQUIREMENT

Only 8 bits of storage space is required for our clone detection system. Our scheme will not increase the number of events in the local database.

B. COMPUTATION WORKLOAD

Tags themselves do not perform any computations. Readers only perform a primitive operation (increment by 1 for the ν-value stored in tags), and the rule verifications are simple and lightweight logical operations.

C. COMMUNICATION COST

While our clone detection scheme requires the reader perform some extra writing operations, it does not inflict any communication overheads with the local databases at the back end. Also, compared with the tailing mechanism by Zanetti, Capcom, and Jules [17], our scheme induces a simpler communication process that needs to update the ν-value (8 bits) only, while the tailing mechanism requires 3 bytes(16 bits for the tail and the pointer and 8 bits for the flag).

VI. CONCLUSION

Conventional clone product detection techniques in RFID-enabled supply chains depend on the global structure of the supply chain or product owes, and thus are insufficient when the fact that supply chains change dynamically is taken into consideration. We proposed a simple yet effective clone detection scheme which overcomes this inadequacy by devising a double-track checking on the consistency of related events. We argue that our work makes the following

contributions:
The simplicity of the proposed scheme yields its independency on the structure of supply chains and thus makes it universally usable.

The double-track verification strategy in the proposed scheme eliminates the overlook of clones that is inevitable in Zanetti's work [15].

The proposed scheme has a competitively high clone detection rate with a reduced communication overhead. As the future work, we plan to investigate scenarios where readers can be hijacked by attackers and business partners may behave illegally. Consumers' privacy protection issue will be focused on as well.

REFERENCES

[1] E. Lefebvre, L. Castro, and L. A. Lefebvre, ``Prevailing issues related to RFID implementation in the healthcare sector,'' in Proc. 10th WSEASInt. Conf. Appl. Comput. Appl. Comput. Sci. (ACACOS), Mar. 2011, 266 272.

a. K. Koscher, A. Juels, V. Brajkovic, and T. Kohno, ``EPC RFID tag security weaknesses and defenses: Passport cards, enhanced drivers licenses, and beyond,'' in Proc. 16th ACM Conf. Compute. Common. Secure., Nov. 2009,33 42.

DOI 10.17148/IJARCCE.2018.7386

[2] J. H. Khor, W. Ismail, and M. G. Rahman, ``Prevention and detection methods for enhancing security in an RFID system," Int. J. Diatribe. SensorNetw., vol. 2012, Jan. 2012, Art. ID 891584.
[3] Z. D. Sun and J. D. Sun, ``RWMS: RFID based weapon management system," in Proc. Int. Conf. Manage., Manuf., Mater. Eng., Jan. 2012, 386 390.
[4] K. Bu, X. Liu, J. Luo, B. Xiao, and G. Wei, ``Unreconciled collisions uncover cloning attacks in anonymous RFID systems," IEEE Trans. Inf.Forensics Security, vol. 8, no. 3, pp. 429 439, Mar. 2013.
[5] M. Lehtonen, F. Michaels's, and E. Fleischer, ``How to detect cloned tags in a reliable way from incomplete RFID traces," in Proc. IEEE Int. Conf.RFID, Apr. 2009, pp. 257 264.
[6] K. Bu, X. Liu, and B. Xiao, ``Fast cloned-tag identification protocols for large-scale RFID systems," in Proc. IEEE 20th Int. Workshop QualityService (IWQ oS), Jun. 2012, pp. 1 4.
[7] T. Staake, F. Thiess, and E. Fleischer, ``Extending the EPC network: The potential of RFID in anti-counterfeiting," in Proc. ACM Symp. Appl.Comput. (SAC), Mar. 2005, pp. 1607 1612.
[8] L. Murkowski and J. Hartnett, ``Deckard: A system to detect change of RFID tag ownership," Int. J. Comput. Sci. Netw. Secur., vol. 7, no. 7, pp. 89 98, 2007.
[9] E.-O. Blass, K. Elkhiyaoui, and R. Molva, ``Tracker: Security and privacy for RFID-based supply chains," in Proc. 18th Annu. Netw. Distrib. Syst.Secur. Symp. (NDSS), Feb. 2011, pp. pp. 1 20.
[10] K. Elkhiyaoui, E.-O. Blass, and R. Molva, ``CHECKER: On-site checking in RFID-based supply chains," in Proc. 5th ACM Conf. Secur. PrivacyWireless Mobile Netw., Apr. 2012, pp. 173 184.
[11] H. S. Lee and H. C. Bang, ``Detecting counterfeit products using supply chain event mining," in Proc. 15th Int. Conf. Adv. Commun.Technol. (ICACT), Jan. 2013, pp. 744 748.
[12] EPC C1G2. [Online]. Available: http://www.impinj.com/, accessed Sep. 1,2014.
[13] EPC C1G2. [Online]. Available: http://www.r dchina.org/, accessedSep. 1, 2014.
[14] D. Zanetti, L. Fellmann, and S. Capkun, ``Privacy-preserving clone detec-tion for RFID-enabled supply chains," in Proc. IEEE Int. Conf. RFID, Apr. 2010, pp. 37 44.
[15] F. Kerschbaum and N. Oertel, ``Privacy-preserving pattern match-ing for anomaly detection in RFID anti-counterfeiting," in Proc. 6thInt. Conf. Radio Freq. Identi cat., Secur. Privacy Issues, Jun. 2010,124 137.
[16] D. Zanetti, S. Capkun, and A. Juels, ``Tailing RFID tags for clone detec-tion," in Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS), Apr. 2013, 1 17.
[17] D. I. Spivak, Category Theory for the Sciences. Cambridge, MA, USA: MIT Press, 2014.
[18] [19] A. Memari, A. Anjomshoae, M. R. Galankashi, and A. R. Bin Abdul Rahim, ``Scenario-based simulation in production-distribution network under demand uncertainty using ARENA," in Proc. 7th Int. Conf. Comput. Converg. Technol. (ICCCT), Dec. 2012,pp. 1443 1448.

DOI 10.17148/IJARCCE.2018.7386