Journal of Computer Science 1(2): 114-120, 2005
ISSN 1549-3636

New RFID System Architectures Supporting Situation Awareness under Ubiquitous Environments

Dongwon Jeong, Young-Gab Kim and Hoh In
Department of Computer Science and Engineering, Korea University
1, 5-ka, Anam-dong, Sungbuk-ku, Seoul, 136-701, Korea

Abstract: Many sensors providing situation data will be in everywhere under the ubiquitous environment. The current RFID system should be extended to recognize and use situation information from the sensors. This study proposes RFID system architectures that are suitable for the ubiquitous environment. This study applies the situation awareness concept to and extends the current RFID system architecture to be able to adapt to the environment. The key components include an inference engine, use policy and definition language. The proposed architecture is named SA-RFID system architecture and can provides the ability to recognize, analyze and use with situation information from sensors under the ubiquitous computing environment. As a result, the usability of the current RFID system is improved and its application increases.

Key words: Radio Frequency IDentification Systgem, Ubiquitous Environment

INTRODUCTION

Radio Frequency IDentification (RFID) system enables contactless information access (read) by use of radio frequency and supports remote monitoring and transactions processing without human's intervention. The RFID is prevalent in various applications such as transportations, electronic cash and logistics and so on [1, 2, 3].

It is estimated that change of computing paradigm and development of technologies will require more extensive and far-reaching usability than the current RFID systems. Especially, many sensors will be able to provide various and abundant situation information in ubiquitous computing environment considered as the next-generation computing environment [4-6]. The utilization of the RFID technologies in such various applications requires functional extension of the current RFID system, which has some limitations. The functions of the current RFID system are limited only to identification and recognition of objects. Thus, the current systems provide the functions for simply reading and processing ID information in little consideration of situations.

For instance, it is assumed that information on a particular RFID tag is used only within a specific time or at a specific place. Current RFID system architecture does not consider such a use policy at all. For the ubiquitous computing environment, it is sometimes needed to receive information from sensors detecting location information and to determine availability of an object identified from the tag at a specific time. Valid geographic location information should be received from the sensor for the access permission. If the location information is not valid or is not received from the sensor and it is not the specific time, the access is not permitted.

A new extended RFID system architecture should be defined for determining and utilizing various use policies for the RFID system based on information acquired from the diverse sensors. The definition of the extended RFID system architecture requires methods to interpret and define the situation information and also needs to consider how to manage the information from the various sensors.

In this study, we propose a Situation-Aware (SA) RFID system architecture which is suitable for ubiquitous computing environment. The proposed system architecture is basically extended the current RFID system architecture and consists of four components. Also it can be distributed into four types according to roles of each component.

General RFID System Architecture: The RFID system is a wireless sensor chip and consists of three main components. The three main components of the RFID system is a RFID transponder (RFID-T) storing information called RFID tag (RFID-T), a RFID reader (RFID-R) capable of reading data from and writing data to the transponder and a Data Processing Subsystem (DPS). The DPS consists of a host computer utilizing data acquired through the RFID-R and applications.

The current RFID system provides limited functions and can be utilized in restricted environment. In future, the ubiquitous computer environment will require a variety of applications and utilizations of the RFID system. This requirement needs information sharing of sensors based on sensor network technology, situation

aware and determination functions and other related technologies ranging to appropriate and effective action processing.

Situation-Aware Technology: Recently, ubiquitous computing(ubiComp), which is considered as a new computing paradigm, is accessible to networks anywhere and anytime [5]. For such an environment, characteristics such as Situation-Awareness, Ad-hoc communication must be provided [5].

Situation-Awareness (SA) analyzes and examines relationship between actions and multiple contexts in view of time changes. Namely, SA means that devices are able to take actions automatically and timely depending on situations. For instance, if a user wearing a watch or a glasses having embedded RFID tag gets up in the morning, the boiler is automatically operated to supply hot water and the electric light is also automatically turned on. When the user is in the bathroom during these automations, the electric light is turned off. After the user comes out of the bathroom, the boiler stops supplying the hot water and the electric light is turned on. These successive processes are performed depending on situations, not at a certain time interval. Not that the actions are processed depending on time, place, or the user behavior, but that the actions are processed through the situation awareness and inference.

The RFID system needs language and architecture for providing the SA technology and enhancing its utility.

Use policy of SA-RFID System: We discuss a management method of the situation-based use policy for sake of valid access management on RFID tag information of the SA-RFID system. The SA-RFID system for the ubiquitous computing environment requires the development of sensor network technology and network technology for high-rate communication and integration of situation awareness technology. Now that the ubiquitous computing environment requires various use policies for the current RFID system, simple reading operation of the current RFID tag information is insufficient to satisfy that requirement.

Appropriate operations need to be allowable using situation information from adjacent sensors and information from the RFID tag. The implementation of the situation-based use policy requires the following technologies.

* Use policy definition and representation method: How to define and represent the use policy depending on situation.
* Inference and actions determination: Inference engine for determining valid actions, that is, authorization for using based on collected situation information.

To address the first requirement, we propose pSA-ID language (pico SA-IDL) on the basis of five W's and one H (5W/1H), basically used by human for situation determination. We leave the second requirement as a further study.

Figure 1 depicts concepts of the pSA-IDL. The pSA-IDL is classified into a user (WHO) policy, an access location (WHERE) and access time (WHEN) policy, an access purpose (WHY) policy, an accessible valid information (WHAT) policy and an access method (HOW) policy. The pSA-IDL has been modified fit for the RFID system in the ubiquitous computing environment, so as to handle complexity of SA-IDL proposed in [6].

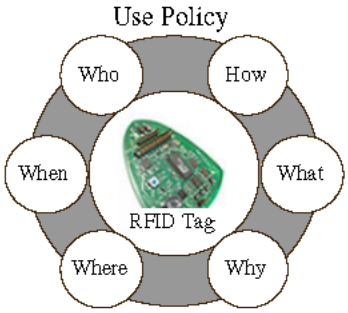

Fig. 1: Concept of pSA-IDL

Figure 2 systematically represents general concept of the pSA-IDS based on 5W/1H by a formal language Z. In Fig. 2, the pSA-IDL includes six attributes for the representation of the use policies in the SA-RFID system. Each attribute may consist of mandatory attributes or optional attributes according to applications. WHO and WHAT policies, that is, who and what attributes are defined as mandatory attributes. Accordingly, who and what attributes have to contain more than one element excluding an empty set. Characteristics of the attributes may be defined variously depending on environment and applications.

pSA-IDL
who: PowerSet WHO= {who1, who2, …}
when: PowerSet WHEN={before, after, now, 9:30, …}
where: PowerSet WHERE={lab, seoul, {(10,10),(100,200)}, …}
why: PowerSet WHY={why1, why2, …}
what: PowerSet WHAT={what1, what2, … }
how: PowerSet How={read_only, write, store, … }
Who ≠ { }, What ≠ { }

Fig. 2: Basic Structure of pSA-IDL

Let's assume that we want to access of product information to be blocked by users of a previous process after a certain process in Supply Chain

Management (SCM) [7]. Provided that a subject of the current access is a 'Retailer' and the information accessibility of the 'Retailer' is limited to an original information, use policy WHO of pSA-IDL is represented as below:

```
situation Retailer{
definition:
        who: Retailer
task:
                who: SCM;
                what: producing_district_information;
                when: now;
                doing: read;
        }
```

The defined pSA-IDL is divided into a definition and task part. The definition part defines a subject being monitored for the SA and the task part describes permitted authorization scope and actions. The above definition language means that the subject is a retailer and the target object is SCM. Also the definition shows the retailer can access (read) information of SCM.

Alternatively, privacy protection policy depending on RFID tag information may be defined as the use policy. Wang *et al*. [8] defines invasion types for the privacy protection policy as follows: Improper access, improper collection, improper monitoring, improper analysis, improper transfer, unwanted solicitation, improper storage. By accepting the above invasion types, how to use personal information relating to the RFID tag is represented in HOW and its access methods are defined as below:

* Access to personal information resource.
* Collection of the personal information resource, or, collection of personal information using the personal information resource.
* Monitoring on the personal information resource, or, monitoring using the personal information resource.
* Analysis on the personal information resource, or, analysis using the personal information resource.
* Transferring of the personal information resource, or, transferring of the personal information.
* Storing of the personal information resource.
* Solicitation of service object.

These access methods are represented in the pSA-IDL as below:

```
situation Retailer{
definition:
        who: Retialer
task:
        who: SCM;
        what: producing_district_information;
        when: now;
        doing: read;
        }
```

The retailer can only access (read) to information on items purchased by the consumer and cannot monitor, collect, delivery, transfer, or store the information. As shown in the above example, the usability of the RFID system is elevated because of assigning various use policies of the RFID tag.

Definition and Classification of SA-RFID System

SA-RFID System Definition: The SA-RFID system, which is suitable for the ubiquitous computing environment, enhances usability of the RFID system by use of information acquired from various sensors. For easy understanding of the SA-RFID system, the following assumption and situation are given.

<Assumption>

As for the public transportation, sensing technology can support a transportation type and its geographic location information. Each sensor transfers the collected information to other devices through wired or wireless communication.

<Situation>

A given application of the RFID tag is the transportation. A certain RFID tag T1 is a transportation card available for nationwide transportations. P1, the owner of T1, lends the transportation card to his friend P2 and requests to use only for the buses within Seoul.

The current RFID system is incapable of dealing with the above situation. In such a situation, it is necessary to recognize the current transportation card, that is, to obtain the location of the RFID tag and the kind of the transportation to be used. The use of the transportation card is determined based on the obtained location information and the information on the kind of the transportation.

The proposed SA-RFID system is capable of recognizing such a situation and determining the use of the resource based on the recognized situation information. We suggest four types of architectures for the SA-RFID system capable of recognizing the situations and taking suitable actions. Our architectures are expanded from the current RFID system architecture and are defined as adaptable for the upcoming ubiquitous computing environment.

Conceptual Architectures of SA-RFID System: In Fig. 3, a RFID tag (RFID-T) holds ID information of an object and it is the same as the traditional-current RFID-T function. The RFID reader (RFID-R) reads information from the RFID-T. In addition, in case of the SA-RFID system architecture, the RFID-R can provides

extended functions that can acquire situation information from sensors, infer proper actions from the situation information and execute the actions.

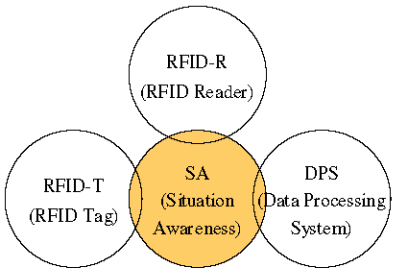

Fig. 3: Conceptual Architecture of SA-RFID System

The data processing system (DPS) basically utilizes the information acquired by the RFID-R. The DPS also contains information pertaining to the use policies and determines suitable actions by inferring and judging the situation information.

For supporting the SA technology, the RFID system requires functions to collect situation information, define use policies with a profitable representation language and infer for determining valid actions using the use policies and the situation information collected. We satisfy these requirements by applying the concept of the SA. The types of the SA-RFID system architecture in this study are selected depending on which components collect and infer the situation information.

Classification of SA-RFID System Architectures: Figure 4 depicts the types of the SA-RFID system architectures classified based on functions for supporting the SA and related operations. The architectures are first classified based on whether a new component is added into the existing RFID system. In other words, the architectures are grouped into a Non SA-Sensor Based (NSSB) architecture not requiring the new component SA-Sensor and a SA-Sensor Based (SSB) architecture requiring the new component. In the NSSB architecture, the SA inference and execution are processed by the DPS (Type I) or by the RFID-R (Type IV). In the SSB architecture, the situation information is inferred by the SA-Sensor but the execution according to the use policies is processed by the SA-Sensor (Type II) or by the DPS (Type III).

As for Type I which extends the functions of the DPS, the situation information is received directly from the sensors and the DPS infers the situation information based on the received situation information and tag information acquired from the RFID-R and executes the resulting actions referred with the use policies. As for Type II, the new component SA-Sensor is added and forwards to the DPS the situation information collected from the sensors. The SA-Sensor infers the situation information from the sensors and sends the results to the DPS. The DPS obtains the tag information from the RFID-R and the actions from the SA-Sensor and then executes the actions. Type III is similar to Type II, the SA-Sensor processes both of the inference and execution depending on the use policies. And the SA-Sensor get the tag information and sends it to the DPS with the action result. Last, as for Type IV, which is an extended architecture that the RFID-R performs the functions of the SA-Sensor. Therefore, the RFID-R processes the inference and execution by collecting the situation information from the sensors.

Characteristics of SA-RFID System Architectures: This section details roles and characteristics of each component in the classified SA-RFID system architectures.

Type I: SA-DPS Based System Architecture: Figure 5 illustrates the SA-DPS based RFID system architecture. When the RFID-R receives the information read from the RFID-T, the SA-DPS also receives situation information from neighboring sensors. Thus, the SA-DPS has to open communication channels to the sensors as well as the RFID-R so as to receive both of information. Since the DPS alone is extended to generate the SA-DPS, it is easy to extend the existing RFID system architecture. Namely, we should only consider the communication issue between SA-DPS and sensors to achieve the SA-RFID system.

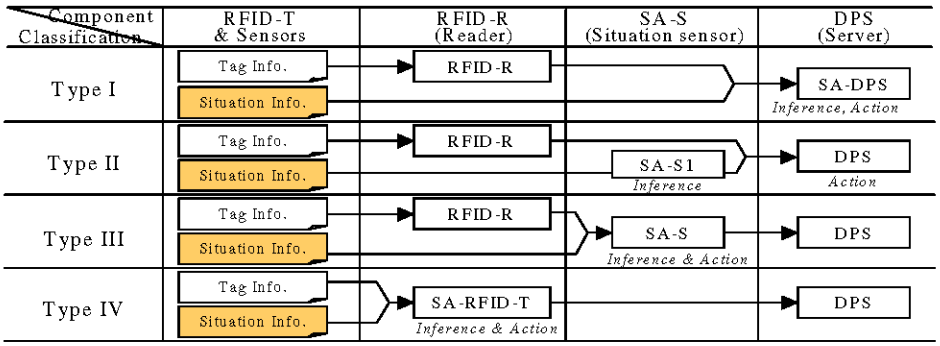

Fig. 4: Classification of SA-RFID System Architecture

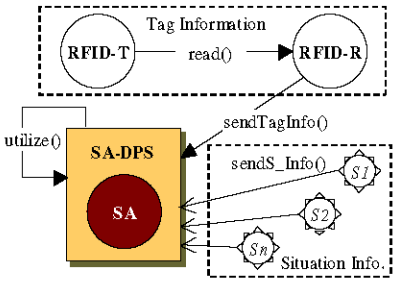

Fig. 5: SA-DPS Based RFID System Architecture

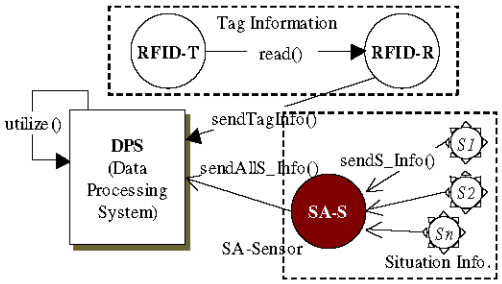

Fig. 6: SA-sensor Supplementary RFID System Architecture

However, this architecture is disadvantageous with respect to accuracy of the situation information and communication reliability owing to the remote communication between the sensors and the SA-DPS. These drawbacks basically result from spatial heterogeneity between the sensor collecting the situation information and the SA-DPS receiving the situation information. To solve the problem due to the directly remote communication between the SA-DPS and the sensors, it is satisfied that all sensors can communicate remotely together with the communication reliability. This issue is out of the scope of this study, which will be not dealt with. The first architecture Type I is advantageous in easy and simple extension, but disadvantageous in requiring additional communication with the RFID-R due to the remote communication function of the sensors.

Type II: SA -Sensor Supplementary Architecture: The second SA-RFID system architecture Type II requires an additional component, the SA-Sensor, for collecting and transferring the situation information from the sensors to the DPS.

Figure 6 illustrates the second SA-RFID system architecture. The RFID-R forwards the tag information from the RFID-T to the DPS. Simultaneously, the SA-Sensor collects situation information from neighboring sensors and then it infers the situation information and transfers the results to the DPS. The DPS determines and executes the use policies based on the tag information from the RFID-R considering the results from the SA-Sensor. This second SA-RFID system architecture is named SA-Sensor supplementary architecture.

As compared with the SA-DPS based system architecture (Type I), the SA-Sensor supplementary architecture performs the read of the RFID-T and the situation information collection of the sensors at the same spatial spot. Hence, the situation information maintains better accuracy and the communication reliability is elevated because the remote communication function is not essentially required to the sensors.

As a result, the SA-Sensor supplementary architecture can reduce overhead on the direction communication with the sensors, as in the SA-DPS based architecture. On the other hand, because the SA-Sensor should be added into the existing architecture, it causes additional cost and more complexity of the system architecture.

Type III: SA-Sensor Oriented Architecture: As for SA-Sensor oriented architecture (Type III) similar to the SA-Sensor supplementary architecture, the newly added SA-Sensor performs both of collecting situation information from sensors and transferring the acting results to the DPS. The difference lies in that Type II has the advanced SA-Sensor. Thus, the advanced SA-Sensor not only infers the situation information but also executes the inferring results, actions, depending on the use policies. Therefore, communication traffic between the SA-Sensor and the server (DPS) decreases and also communication cost is productive.

Figure 7 illustrates this SA-Sensor oriented RFID system architecture. In this SA-Sensor oriented architecture, the RFID-R requires only local communication with the SA-Sensor, not remote communication with the DPS as in the SA-Sensor supplementary architecture. Consequently, error probability due to the remote communication decreases. And also transfer reliability increases. In addition, the overhead that the RFID-R has the remote communication function is mitigated.

Meanwhile, the SA-Sensor is separately required to thus leave cost problem behind. Sufficient and powerful resource and computing capability is required because the SA-Sensor performs both of situation inference and execution.

Type IV: SA-RFID Reader Based Architecture: Type IV is a type that the RFID-R function of the general RFID system architectures is extended. Concretely, the RFID-R collects situation information from sensors, analyzes and infers situation information and executes the results including the traditional function that is to read the RFID tag information. We name such a RFID-R as SA-RFID reader and such an architecture as SA-RFID reader based RFID system

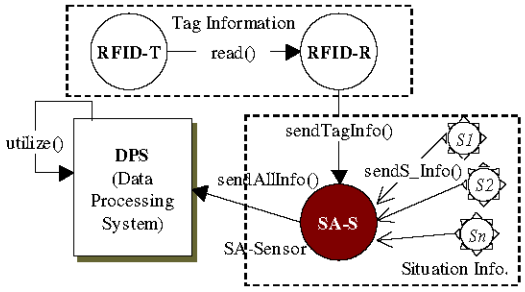

Fig. 7: SA-Sensor Oriented RFID System Architecture

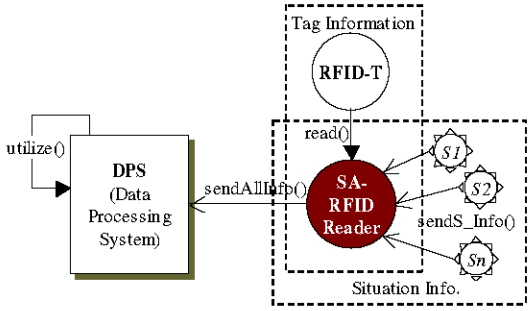

Fig. 8: SA-RFID Reader Based RFID System Architecture

architecture. Figure 8 illustrates the SA-RFID reader oriented RFID system architecture.

The SA-RFID reader based architecture maintains the basic architecture of the existing RFID system without adding a new component as in the SA-DPS based oriented architecture and extends the function of the RFID-R. Accordingly, the extension to the SA-RFID system is simple and the its architectural complexity is not considerably high as compared with the SA-Senor based architecture. This architecture supports channel consistency since the single component (SA-RFID reader) reads the RFID tag information as well as collects the situation information from sensors.

However, this architecture requires that the RFID-R should be equipped for additional functions such as remote communication with the DPS, communication with sensors, situation information collection and so forth. Thus, the RFID-R experiences more overhead than the other architectures.

Evaluations: Table 1 organizes comparisons on advantages and disadvantages of the architectures. As to the development of the SA-RFID system by extending the existing RFID system, Type I is superior to the other types because Type I employs the existing RFID system as it is. In comparison, Type II and Type III, which require the new component SA-Sensor, have lower extensibility than the others.

As to the accuracy of the collected situation information, all sensors remote-communicate directly with the DPS in Type I. That is, the DPS and the sensors, which collect the situation information, are not present at the same spot. Hence, Type I has higher error probability with respect to the collected situation information than the others. Moreover, Type I has lower performance in the communication cost increase and the communication reliability problem. The other architectures collect the situation information at the same spot and have higher accuracy than Type I. Particularly, since the RFID-R of Type IV is responsible for collecting situation information from various sensors, Type IV has the highest accuracy of information. Type I, Type II and Type III require additional communications between the DPS and the sensors, between the RFID-R and the SA-Sensor and between the DPS and the RFID-R. Type I incurs high communication cost due to the direct communications with all sensors. In case of Type II, the RFID-R and the SA-Sensor respectively remote-communicates with the DPS. Type III additionally requires the local communication between the RFID-R and the SA-Sensor as compared with Type IV. As a result, Type IV provides optimum performance in the light of the communication cost and the reliability. We will leave quantitative evaluations on these architects for further researches.

Table 1: Comparisons of SA-RFID System Architectures

Types Items	Type I: SA-DPS based	Type II: SA-S Supplementary	Type III: SA-S Oriented	Type IV: SA-RFID Reader
Extensibility	> [The others]	New comp. required	New comp. required	[Type I] <
Accuracy of situation info.	< [The others]	> [Type I]	> [Type II]	> [The others]
Communication cost	> [The others]	> [Type III]	> [Type IV]	< [The others]
Communication reliability	< [The others]	< [Type IV]	< [Type IV]	> [The others]
System building Cost	Depending on remote Communication cost	Depending on cost to add the SA-Sensor	Depending on cost to add the SA-Sensor	Depending on the RFID reader

CONCLUSION

Ubiquitous computing is considered as the next generation computing paradigm. Many sensors will be able to provide various and abundant situation information in the ubiquitous computing environment. Such a change of computing paradigm and development of technologies will require more extensive and far-reaching usability than the current RFID systems. Currently, the functions of the current RFID system are limited only to identification and recognition of objects. Thus, the systems provide the functions for simply reading and processing ID information in little consideration of situations.

In case that information on a RFID tag is used only within a specific time or at a specific place, current RFID system architecture does not consider such a use policy at all. To support this application, it is sometimes needed to receive information from sensors detecting location information and to determine availability of an object identified from the tag at a specific time. Valid geographic location information should be received from the sensor for the access permission. Therefore, a new extended RFID system architecture should be defined for determining and utilizing various use policies for the RFID system based on information acquired from the diverse sensors. The definition of the extended RFID system architecture requires methods to interpret and define the situation information and also needs to consider how to manage the information from the various sensors.

We proposed the use policies and a formal language for the expression of the use policies to support the SA concept in the ubiquitous computing environment, suggested several types of SA-RFID system architecture. Finally, we qualitatively compared and evaluated the system architectures. Our system architectures may be selectively utilized as need. It is expected that our architectures overcome simple and restrained functions of the existing RFID system and provide far-reaching applications. Above all, it is feasible to utilize the various RFID tags based on the situation information and determine the diverse access methods.

Further researches are demanded on implementation technologies of optimum inference engines. Especially, the compactness of the inference engines allows the definition on more diverse system architectures beyond our system architectures.

REFERENCES

1. Finkenzeller, K., 2000. RFID Handbook: Radio-Frequency Identification Fundamentals and Applications. John Wiley and Sons.
2. Sarma, S.E., S.A. Weis and D.W. Engels, 2002. RFID systems and security and privacy implications. Lecture Notes in Computer Science, In Workshop on Cryptographic Hardware and Embedded Systems, LNCS 2523, February, pp: 454-470.
3. Association for Automatic Identification and Mobility (AIM), http://www.aimglobal.org/
4. Yau, S., F. Karim, Y. Wang, B. Wang and S. Gupata, 2002. Reconfigurable context-sensitive middleware for pervasive computing. IEEE Pervasive Computing, 1: 33-40.
5. Yau, S.S. and F. Karim, 2002. Adaptive middleware for ubiquitous computing environments. Proc. IFIP 17th WCC, August.
6. Yau, S., Y. Wang and F. Karim, 2002. Developing situation-awareness in middleware for ubicomp environments. Proc. 26th Intl. Computer Software and Applications Conference, pp: 233-238
7. Daugherty, P.J., T.P. Stank and D.S. Rogers, 1996. Third-party logistics service providers: Purchasers' perceptions. The J. Supply Chain Management, 32: 23-29.
8. Wang, H., M.K.O. Lee and C. Wang, 1998. Consumer privacy concerns about internet marketing. Communication of the ACM, 41: 63-70.