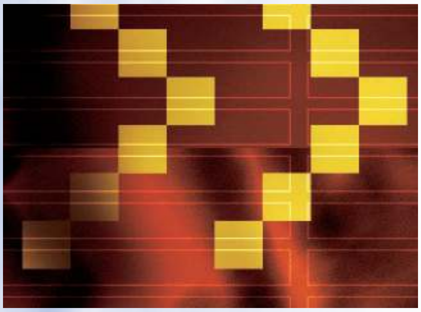
Enabling Next-Generation RFID Applications: Solutions and Challenges



Quan Z. Sheng
University of Adelaide

Xue Li
University of Queensland

Sherali Zeadally
University of the District of Columbia

Radio-frequency identification technology provides promising benefits such as inventory visibility and business process automation. However, if companies are to realize these benefits, researchers must address major challenges such as data processing, integration architecture design, security, and privacy.

The ability to uniquely identify individual objects is essential to many aspects of modern life such as manufacturing, distribution logistics, access control, and fighting terrorism. Radio-frequency identification is a wireless communication technology that is useful for precisely identifying objects.[1] RFID uses radio-frequency waves to transfer identifying information between tagged objects and readers without line of sight (LOS), providing a means of automatic identification.

Although RFID has been around for more than half a century,[2] it began to attract a lot of attention only in recent years due to the convergence of lower cost and the increased capabilities of RFID tags. Currently, RFID is emerging as an important technology for revolutionizing a wide range of applications, including supply-chain management, retail sales, anticounterfeiting, and healthcare.[1,3]

Many organizations are planning to or have already exploited RFID to achieve more automation, efficient business processes, and inventory visibility. For example, Wal-Mart reportedly reduced out-of-stocks by 30 percent on average after launching its RFID program (http://rfidtimes.org/2006/05/17). Predictions indicate that RFID will be worth billions of dollars in new investments. According to IDTechEx, a leading market research and advisory firm, the RFID market will increase from US$4.96 billion in 2007 to US$26.88 billion in 2017 (www.idtechex.com/products/en/view.asp?productcategoryid=119).

While RFID provides promising benefits in many applications, researchers must overcome some major hurdles before these benefits can be realized. An important challenge is managing RFID data, which is noisy, generated dynamically in very large streams, has a limited active lifespan, and possesses useful contextual characteristics such as temporality, spatiality, and implicit semantics.[4,5] The deployment of large-scale RFID applications also introduces unique challenges such as scalability and heterogeneity. Finally, given the ability to inexpensively tag and thus monitor numerous items or people, RFID raises serious security and privacy concerns that inhibit adoption of the technology.[6]

SYSTEM BASICS

An RFID system's main function is automatic identification of objects or persons using radio waves. A typical RFID system consists of

0018-9162/08/$25.00 © 2008 IEEE

- a transponder or tag attached to the objects or persons,
- an interrogator or reader that creates an RF field for detecting radio waves, and
- a computer network to connect the readers.

A tag contains a chip that stores the identifying information of the object or person to which it is attached and an antenna that communicates the information via radio waves. When a tag passes through an RF field that a reader generates, the tag transmits that information to the reader, thereby identifying that object or person. Consequently, there is no LOS requirement for object identification in an RFID system. The reading distance ranges from a few centimeters to more than 300 feet depending on tag type, reader power, interference from other RF devices, and so on.

> **RFID technology has been moving rapidly from a limited number of applications to many new application areas.**

RFID tags are classified by energy source. An *active* tag has its own transmitter and a power source to run the microchip's circuitry and broadcast signals to readers. A *passive* tag does not have its own power source and instead scavenges power from the electromagnetic radiation emitted by readers; it also has an indefinite operational life. *Semiactive* tags use their own power source to run the microchip's circuitry but also scavenge power from the waves sent out by readers to broadcast their signals.[4]

Active and semiactive tags are expensive and typically used for high-value goods or large assets that must be tracked over long distances. For example, the US Department of Defense uses active tags to track many containers being shipped to military bases and units overseas. In contrast, passive tags are inexpensive and can be used for common materials in very large quantities. Currently, significant research efforts are under way to achieve 5-cent tags by shrinking chip size, cutting antenna cost, and increasing tag consumption—for example, to meet RFID mandates from Wal-Mart and the US Department of Defense.

RFID tags have different capabilities, are composed of various materials, and come in many shapes—including key fobs, credit cards, capsules, and pads—and are available in sizes ranging from as small as a grain of rice to as big as a six-inch ruler. The tags can have metal external antennas, embedded antennas, or printed antennas.

RFID APPLICATIONS

During the past few years, RFID technology has been moving rapidly from a limited number of applications—for example, access control and toll collection—to many new application areas.

Industrial and commercial

RFID technology is being deployed in a wide range of industrial and commercial systems, including manufacturing and logistics, retail, animal tracking, and transport and admission ticketing.

An important application in this area is supply-chain management, where RFID helps close information gaps by enabling real-time supply chain visibility. Numerous organizations currently exploit RFID technology to track products from supplier to distribution center, warehouse stock, and point of sale (www.rfidjournal.com/article). The ability to precisely record product movement is also useful for theft prevention, product recall, and anticounterfeiting.

Livestock tagging is becoming a substantial market for RFID, given the rising concern about food safety. For example, many countries now demand that all cattle be RFID-tagged so that they can be tracked in the event of an outbreak of mad cow disease.

RFID technology is widely used for transport and admission ticketing for better service and security. The Hong Kong Octopus transport ticketing system (www.octopuscards.com) is one of the most successful RFID-enabled transportation payment applications; more than eight million people hold the card and use it on all forms of public transport in the city. In 2005, Japan's NTT DoCoMo launched an RFID-enabled mobile phone that can be used as an electronic wallet to make electronic purchases, act as a boarding pass on domestic air flights, and authorize entry through corporate security doors (www.spectrum.ieee.org/nov05/2150).

Entertainment

Several research projects are investigating the exploitation of RFID technology in entertainment applications. For example, San Francisco's Exploratorium uses the RFID-based eXspot system[7] to help visitors interact with exhibits within the science museum, allowing them to register and document their interests, then extend the visit via the Internet after going home.

Healthcare and pharmaceuticals

RFID technology is a promising candidate for reducing operating costs and improving patient safety in the healthcare industry by tracking and monitoring patients, doctors, medical assets, and drugs. For example, Intel's Proactive Health project[8] uses RFID technology to facilitate elder care by monitoring activities such as medication intake.

APPLICATION DEVELOPMENT ISSUES

Many applications use RFID technology and computerized systems such as networking services, databases,

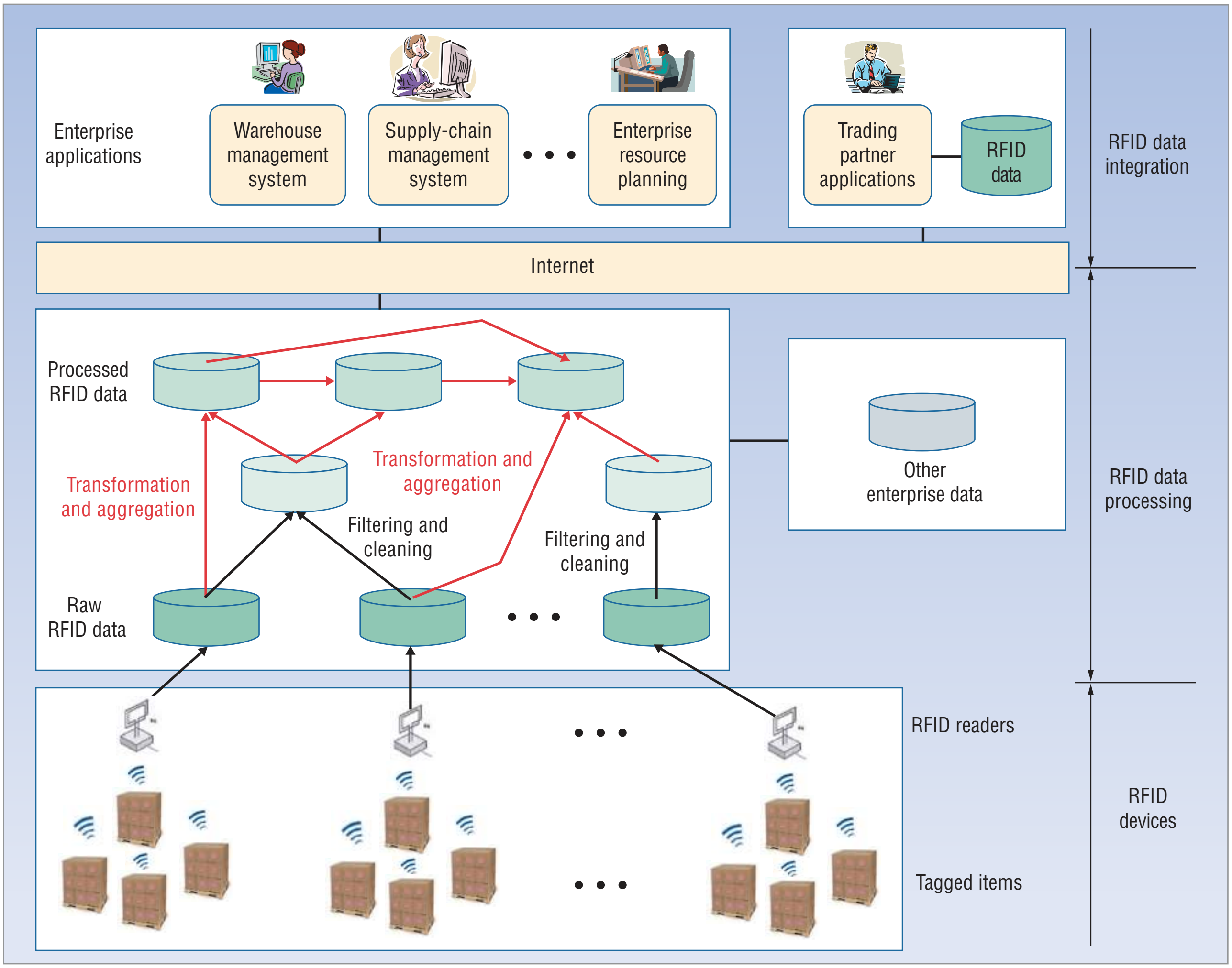


Figure 1. RFID framework architecture. Interactions in RFID applications occur at three layers: devices, data processing, and data integration.

and Web servers to achieve advanced business goals—for example, real-time product tracking.[1]

Figure 1 shows a generic RFID framework. Interactions in RFID applications occur at three layers. The *devices* layer consists of RFID tags and readers as well as RFID protocols—for example, ISO 14443 and Electronic Product Code (EPC; www.epcglobalinc.org/standards) Class 0 and Class 1—for reading and writing RFID data. The *data processing* layer consists of several software components for communicating with RFID readers, filtering and cleaning RFID data, and adapting such data for high-level applications including semantic filtering and automatic data transformation and aggregation. The *data integration* layer consists of applications that exploit local RFID data as well as RFID data coming from outside business entities.

For an organization to achieve a seamless integration of RFID data with business processes, the applications must be able to understand different data semantics. RFID data can be formatted in, for example, Physical Markup Language (http://web.mit.edu/mecheng/pml), and sent to different targets as messages, streams, or other formats via Web services, the Java Message Service, HTTP responses, or TCP/IP data packets.

Data characteristics

RFID data possesses a unique set of characteristics that RFID applications must consider.[4]

Inaccuracy. While current RFID reader accuracy is improving, erroneous readings still occur in RFID systems such as duplicate reads, missed reads, and ghost reads (when an RFID reader "reads" an identifier that is not stored on any tag within the reader's field) due to interference or temporary or permanent malfunction of some component. Therefore, RFID data tends to be noisy and unreliable.

Large-volume streams. RFID data is generated quickly and automatically, and the volume can be enormous. For example, Wal-Mart generates around 7 terabytes of data every day from tags used at the item level.

Temporality and spatiality. RFID data is generated dynamically and is associated with time stamps when

Table 1. RFID data processing approaches.

Platform	Inaccuracy	Large-volume streams	Temporality	Spatiality	Implicit references	Limited active lifespan
Siemens' RFID middleware	Partially addressed: filtering duplicated readings	RFID data partitioning	Dynamic Relationship ER model	Dynamic Relationship ER model	Rule-based data transformation	Considered in RFID data partitioning
SMURF	Declarative, adaptive smoothing filter based on a statistical sampling approach	Not addressed	Not explicitly addressed	Not explicitly addressed	Not addressed	Not addressed
EPC-bitmap	Not addressed	EPC-bitmap data type for a collection of EPCs	Not explicitly addressed	Not explicitly addressed	Not addressed	Not addressed
UIUC's RFID warehousing	Not addressed	RFID-cuboid data structure	Stay table	Stay table	Not addressed	Not explicitly addressed

readings are made. In addition, tagged objects are typically mobile and go through different locations during their life cycle. Temporal and spatial information is important for tracking and monitoring RFID objects. For example, using time stamps, it is possible to track how long it takes an aircraft part to move from the warehouse to the maintenance venue.

Implicit inferences. RFID data always carries implicit information such as changes of state and containment relationships among objects. To use RFID data, applications require the context of other information—such as environmental situations—to make proper inferences. For example, a supply-management system that captures a case of cameras and a pallet together in a packing station could infer that the case is packed in the pallet.

Limited active lifespan. RFID data normally has a limited active life period, during which a given system actively updates, tracks, and monitors the data. For example, in a supply-chain management system this period starts when the manufacturer delivers the products and ends when customers purchase the products.

Data integration

Integrating RFID data with business processes presents many challenges.[9]

Scalability. An important criterion to consider when evaluating RFID integration solutions is scalability, which refers to a system's ability to grow in one or more dimensions—such as the volume of RFID data and the number of transactions—without affecting performance. Organizations that adopt RFID technology must handle data from thousands of readers distributed across various sites.

Heterogeneity. An RFID solution can be deployed across multiple sites, companies, or even countries using different hardware, data structures, and standards. RFID systems must support the distribution of message preprocessing functionality—for example, filtering and aggregation—as well as business logic across multiple nodes to better map to existing company and cross-company structures.[9]

Manageability. Good support of administration and testing is a prerequisite for the successful deployment of an RFID solution in large-scale, distributed applications. RFID systems must facilitate the supervision, testing, and control of their individual components as well as end-to-end processing of RFID data.

Security. The vast amount of potentially sensitive information involved in RFID systems makes security critical.[2] For example, a company that implements RFID in its supply chain does not want competitors to track its shipments and inventory. Further, standard security mechanisms such as the Secure Sockets Layer are resource-consumption intensive and unsuitable in RFID systems involving other CPU-intensive work such as filtering. Sophisticated security measures must be in place to ensure the safe protection of RFID applications.

Openness. System interoperability is another important parameter in RFID data integration. For instance, a well-designed reader adapter at the edge server makes RFID integration reader-agnostic. In addition to being hardware-agnostic, RFID systems should be based on existing communication protocols such as TCP/IP and HTTP as well as syntax and semantics standards such as XML, PML, and EPC. An open RFID architecture will allow use of RFID devices from a wide array of hardware providers and, more importantly, support the deployment of RFID solutions across institutional or country boundaries.

DATA PROCESSING APPROACHES

Due to its unique characteristics, RFID data must be appropriately processed before an application can use it. Table 1 compares representative research work on RFID data processing in industry and academia.

Siemens' RFID middleware

Siemens' proposed RFID middleware system[5] uses Dynamic Relationship ER, an expressive temporal-based data model, to represent RFID data. DRER abstracts a set of entities—namely object, reader, location, and transaction—and models the interactions between them as either state- or event-based relationships. For state-based relationships, the associated attributes `tstart` and `tend` represent the relationship's lifespan—for example, the period that a product stays in the warehouse. For event-based relationships, an associated attribute time stamp indicates when the event occurred. Maintaining the temporal and spatial history of RFID objects makes it easy to track and monitor them—for example, searching for missing items.

SMURF

UC Berkeley's Statistical Smoothing for Unreliable RFID data[10] is an adaptive smoothing filter for cleaning raw RFID data streams. By viewing and thereafter modeling RFID data streams as a random sample of the tags in the physical world, SMURF exploits a statistical-sampling-based approach to balance reader unreliability (such as missed readings) and tag dynamics (tag movements in and out of the reader's detection field) in the data cleaning process. The ability to automatically determine the right smoothing window size and continuously adapt it based on the observed readings makes it easier to integrate SMURF with RFID middleware platforms to provide reliable RFID data.

RFID data must be appropriately processed before an application can use it.

EPC-bitmap

Oracle's EPC-bitmap[11] is a novel data type for efficiently handling high-volume RFID data generated from item-level tracking applications. Most such applications can track tagged items in groups based on their location, expiration date, manufacturer, or other shared properties. An EPC-bitmap represents a collection of EPCs with common segments such as header, manager number, and object class, and the application can access and manipulate it using a set of EPC-bitmap operations—for example, epc2bmp and bmp2epc for conversion. This approach achieves significant storage savings, while query performance remains the same as or better than traditional database systems that natively store EPC collections.

UIUC's RFID warehousing

Researchers at the University of Illinois at Urbana-Champaign (UIUC) have proposed a novel model[12] for warehousing RFID data that exploits the tendency of individual objects to move and stay together, making it possible to collapse multiple movements of RFID objects into a single record without loss of information. The model consists of a hierarchy of highly compact summaries, represented as RFID-cuboids, of data aggregated at different abstraction levels where analysis takes place. Each RFID-cuboid records object movements and stores product information for each RFID object, information on objects that stay together at a location, and path information necessary to link multiple stay records. The proposed model results in smaller database sizes and provides efficient support for a wide range of RFID queries.

DATA INTEGRATION PLATFORMS

Major software vendors such as Sun Microsystems, SAP, BEA Systems, and IBM, as well as research organizations including the UCLA-based Wireless Internet for the Mobile Enterprise Consortium (WINMEC), Auto-ID Labs, and Siemens Research are currently working on RFID data integration. Table 2 compares some of the major platforms. Note that for commercial products, our analyses are based on user manuals and white papers as there are few or no technical publications detailing those products.

WinRFID

UCLA's WinRFID (www.wireless.ucla.edu/rfid/winrfid), a middleware system that enables rapid RFID application development, consists of five main layers.

The *physical* layer includes the hardware consisting of readers, tags, and other sensors. The *protocol* layer abstracts the reader-tag protocols. The *data processing* layer processes the data streams the RFID reader network generates. The *XML framework* and *data presentation* layers handle data representation and presentation, respectively.

Currently, a Web-service-based distributed architecture is under development. To support extensibility, WinRFID exploits the .NET framework's runtime plug-in feature. New readers, protocols, and data transformation rules can be added into corresponding modules with minimum disruption of the existing infrastructure. A rule-based engine handles data filtering, aggregation, and adaptation.

SAP AII

SAP's Auto-ID Infrastructure[9] is middleware that integrates data from RFID devices with enterprise applications. SAP AII is built on SAP's Web Application Server, which is part of the company's NetWeaver (www.sap.com/solutions/netweaver) integration and application platform.

The SAP AII architecture consists of four layers. The *device* layer supports different types of sensor devices

Table 2. RFID data integration platforms.

Platform	Scalability	Heterogeneity	Manageability	Security	Openness
WinRFID	Self-contained, distributed middleware modules	Abstracted protocol module for published RFID protocols and XML framework for data representation	WinRFID management console	Authentication and access restriction support of RFID data	Standards-based framework (for example, Web services, XML)
SAP AII	Distributed device controllers and Auto-ID nodes	Hardware-independent device interface, distributed Auto-ID nodes	Auto-ID administrator, tools for simulating and testing RFID messages and readers	Not addressed	Compliant with proposed EPCglobal standards
EPCglobal Network	Distributed EPCIS, centralized discovery service	EPC-compliant devices	Not explicitly supported	Under development	Standards-based framework such as Web services and XML-based PML
Sun Java System RFID Software	Distributed architecture of the RFID event manager	Extensible device adapters	Browser-based interface for centralized monitoring and management of devices and services	Security services in Java Enterprise System	Standards-based, service-oriented architecture (SOA)
BEA WebLogic RFID	Lightweight, distributed architecture for RFID edge servers	Out-of-box support of major RFID readers, SOAP interfaces	Administration console, monitoring and management agent, reader simulator	Not addressed	Standards compliance (for example, EPCglobal and ISO standards), SOA
WebSphere RFID server	WebSphere RFID Device Infrastructure (only devices embedded with the infrastructure)	Not addressed	Offers system management capabilities like management and monitoring of hardware and applications in remote locations	Not addressed	Standards-based framework

via a hardware-independent low-level interface. The *device operation* layer contains one or more device controllers, coordinating multiple devices. The *business process bridging* layer associates observation messages with existing business processes, realized by an Auto-ID node component. The *enterprise application* layer supports business processes such as customer relationship management. To allow RFID application testing without installing physical devices, SAP AII also provides tools for simulating readers and messages.

EPCglobal Network

The EPCglobal Network, often referred to as the "Internet of things," was developed by the Auto-ID Center and EPCglobal (www.epcglobalinc.org), a not-for-profit organization that supports worldwide adoption and standardization of EPC technology. The framework seeks to realize a data-on-network system in which RFID tags containing an unambiguous ID (EPC) and other data pertaining to objects is stored on and accessible over the Internet.

Major components include the Object Naming Service (ONS), which provides references to saved object information to facilitate discovery, and the EPC Information Service (EPCIS), which offers an interface for accessing stored RFID data.

Information on the movement of RFID objects must be continuously published to a centralized discovery service for tracking purposes, which unfortunately prevents the EPCglobal Network from realizing a full-fledged distributed architecture.

Sun Java System RFID Software

Sun Java System RFID Software (www.sun.com/software/jini/news/Jini_RFID_Profile_Final.pdf) is one of the first RFID integration platforms focusing on large-scale deployments. Its service-oriented architecture provides network services to applications through several standard protocols and interfaces.

Java System RFID Software consists of two major components: The *event manager* processes (filters and aggregates) RFID data, while the *information server* provides access to the business events generated by the event manager and serves as an integration layer that offers options for integrating with enterprise applications.

BEAWebLogic RFID

BEA Systems' BEAWebLogic RFID, which "delivers the first end-to-end, standards-based RFID infrastructure platform designed to automate new RFID-enabled business processes" (www.bea.com/framework.jsp?CNT=index.htm&FP=/content/products/weblogic/rfid), consists of three main products. Edge Server is lightweight software that can be deployed at various sites to filter, integrate, and disseminate RFID data as well as monitor and configure RFID readers; Enterprise Server centrally manages RFID data collected from RFID edge servers; and Compliance Express is designed to meet current compliance challenges while establishing a foundation for future expansion.

> **RFID integration platforms must support legacy software systems.**

WebSphere RFID

IBM's RFID solution includes three components: RFID devices, WebSphere Premises Server (www-306.ibm.com/software/integration/premises_server/index.html), and WebSphere Business Integration Server. RFID devices must be embedded with the WebSphere RFID Device Infrastructure, software that supports functions for RFID data collection and delivery. The Premises Server is middleware that aggregates, monitors, interprets, and escalates RFID data and provides an interface for integration with enterprise applications.

OPEN RESEARCH ISSUES

Despite much progress in RFID data processing and integration, many research challenges remain open.

Accurate and reliable data provisioning

Because RFID-enabled applications primarily use RFID data to automate business processes, inaccurate data could misguide application users.[4,10] For example, a ghost read at a check-out point might trigger a charge to a customer who is not purchasing the corresponding goods. Extensive research is needed to improve RFID data reliability.

Efficient data management

Because RFID systems can generate large volumes of data,[4] accumulation of RFID data can easily lead to poor performance such as slower queries and updates. Current solutions for efficient RFID data management use a data-mining-based approach[11,12] that assumes data shares some common properties—for example, moving together in bulk mode or having the same expiration date—and can be grouped based on such properties. However, these solutions are limited to applications such as supply-chain management; a more general approach is needed for handling massive RFID data. Given the limited active lifespan of such data, novel mechanisms such as partitioning of RFID data will become increasingly important.

Intelligent data transformation and aggregation

Raw RFID data presents little value until it is transformed into a form suitable for application-level interactions. Moreover, such data has implicit meanings and associated relationships with other RFID data—for example, containment—about which applications must make appropriate inferences.[4] For example, observations of two items and a case in a certain time interval can imply that the items are packed in the case. Projects such as UC Berkeley's HiFi data management infrastructure (http://hifi.cs.berkeley.edu/home/about.html) use event modeling techniques to formulate relationships among objects for RFID applications.

Large-scale application support

Developing and deploying large-scale RFID applications such as nationwide supply-chain management remains a challenge. Although some platforms support the distribution of functionalities such as RFID edge processing, a full-fledged distributed architecture for sharing and synchronizing data across multiple nodes is needed.

Deploying a large distributed system also requires the ability to continuously monitor the state of the system and adaptively adjust its behavior. Given the large number and highly distributed nature of RFID devices, administration tools for visualizing, configuring, testing, and monitoring RFID devices and system components will become increasingly important.

Seamless integration of legacy systems and sensors

RFID integration platforms must support legacy software systems. Such systems are normally mature, heavily used, and constitute massive corporate assets, thus replacing them with new systems is too costly.

Vendors and researchers are currently developing middleware that links new RFID systems into existing infrastructures. They are also working on ways to integrate sensors with RFID tags to obtain information about the physical world as well as objects' identity.[3] For example, a sensor-enabled RFID tag attached to an airplane part could record the stress and shock experienced during a flight, which could be used to make the corresponding preventive maintenance schedule.

Security

High-security applications such as access control, electronic passports, and systems for making payments or issuing tickets are increasingly using RFID. To adopt such applications, businesses must be confident that their data is safe. Researchers have proposed a few strategies to authenticate and encrypt RFID data,[2] but doing so increases the resource consumption and latency of read cycles. Comprehensive solutions are needed not only to protect RFID information but also to maintain desirable system performance.

Privacy

Privacy is generally misperceived as an issue for which the natural solution consists of good security mechanisms. Although security and privacy are tightly interrelated, securing RFID applications does not necessarily ensure privacy.

Two notable privacy concerns in RFID applications are their potential to leak personal property information and their ability to track consumers' spending history and physical whereabouts.[6] For example, terrorists could scan digital passports to target specific nationalities, and police could abuse a convenient new means of cradle-to-grave surveillance.

To address privacy threats for RFID users, researchers must implement technical solutions such as RSA blocker tags[6] as well as legal countermeasures[13] to ensure consumers that their data will not be misappropriated.

In recent years, RFID has become a vibrant and rapidly expanding area of research and development. The technology's ability to precisely identify objects at low cost and without LOS creates many new and exciting opportunities for applications that could become an integral part of our daily lives. To develop and deploy these applications, however, researchers first must find robust, scalable, secure solutions to the unique challenges of RFID data that meet the specific requirements of system architectures. ■

Acknowledgment

This research is partially supported by the Australian Research Council Discovery Grant DP0878917.

References

1. B. Nath, F. Reynolds, and R. Want, "RFID Technology and Applications," *IEEE Pervasive Computing,* vol. 5, no. 1, 2006, pp. 22-24.
2. M.R. Rieback, B. Crispo, and A.S. Tanenbaum, "The Evolution of RFID Security," *IEEE Pervasive Computing,* vol. 5, no. 1, 2006, pp. 62-69.
3. G. Borriello, "RFID: Tagging the World," *Comm. ACM,* vol. 48, no. 9, 2005, pp. 34-37.
4. S.S. Chawathe et al., "Managing RFID Data," *Proc. 30th Int'l Conf. Very Large Databases* (VLDB 04), VLDB Endowment, 2004, pp. 1189-1195.
5. F. Wang and P. Liu, "Temporal Management of RFID Data," *Proc. 31st Int'l Conf. Very Large Databases* (VLDB 05), VLDB Endowment, 2005, pp. 1128-1139.
6. M. Ohkubo, K. Suzuki, and S. Kinoshita, "RFID Privacy Issues and Technical Challenges," *Comm. ACM,* vol. 48, no. 9, 2005, pp. 66-71.
7. S. Hsi and H. Fait, "RFID Enhances Visitors' Museum Experience at the Exploratorium," *Comm. ACM,* vol. 48, no. 9, 2005, pp. 60-65.
8. E. Dishman, "Inventing Wellness Systems for Aging in Place," *Computer,* May 2004, pp. 34-41.
9. C. Bornhövd et al., "Integrating Automatic Data Acquisition with Business Processes: Experiences with SAP's Auto-ID Infrastructure," *Proc. 30th Int'l Conf. Very Large Databases* (VLDB 04), VLDB Endowment, 2004, pp. 1182-1188.
10. S.R. Jeffery, M.J. Franklin, and M. Garofalakis, "An Adaptive RFID Middleware for Supporting Metaphysical Data Independence," *VLDB J.,* vol. 17, no. 2, 2008, pp. 265-289.
11. Y. Hu et al., "Supporting RFID-Based Item Tracking Applications in Oracle DBMS Using a Bitmap Datatype," *Proc. 31st Int'l Conf. Very Large Databases* (VLDB 05), 2005, pp. 1140-1151.
12. H. Gonzalez et al., "Warehousing and Analyzing Massive RFID Data Sets," *Proc. 22nd Int'l Conf. Data Engineering* (ICDE 06), IEEE CS Press, 2006, p. 83.
13. K.C. Jones, "California Senate Approves Bill to Outlaw Skimming RFID Tags," *InformationWeek,* 31 Jan. 2008.

Quan Z. Sheng *is a lecturer in the School of Computer Science at the University of Adelaide. His research interests include Web services, business process integration, data integration, and pervasive computing. Sheng received a PhD in computer science from the University of New South Wales. He is a member of the IEEE and the ACM. Contact him at qsheng@cs.adelaide.edu.au.*

Xue Li *is a senior lecturer in the School of Information Technology and Electrical Engineering at the University of Queensland. His research interests include data mining, multimedia data security, database systems, and intelligent Web information systems. Li received a PhD in information systems from the Queensland University of Technology. He is a member of the IEEE and the ACM. Contact him at xueli@itee.uq.edu.au.*

Sherali Zeadally *is an associate professor in the Department of Computer Science and Information Technology at the University of the District of Columbia, Washington, D.C. His research interests include computer networks, mobile computing, RFID, network and system security, and ubiquitous computing. Zeadally received a PhD in computer science from the University of Buckingham, England. He is a Fellow of the British Computer Society and the Institution of Engineering and Technology. Contact him at szeadally@udc.edu.*