

Secure Sharing of Item-level Data in the Cloud

Florian Kerschbaum
SAP AG, SAP Research Center Karlsruhe
Vincenz-Prießnitz-Str. 1, 76131 Karlsruhe, Germany
florian.kerschbaum@sap.com

Leonardo Weiss Ferreira Chaves
SAP AG, SAP Research Center Karlsruhe
Vincenz-Prießnitz-Str. 1, 76131 Karlsruhe, Germany
leonardo.weiss.f.chaves@sap.com

Abstract—Companies can optimize their supply chain if they exchange item-level data, i.e. specific data about each item gathered with the help of Radio Frequency Identification or 2D bar codes. However, business critical information might be inferred from this data, e.g. strategic relations or best practices. Therefore, companies are reluctant to share item-level data.

In this paper we discuss requirements for an encryption scheme for exchanging item-level data by storing it in a cloud-based data repository. We envision a system that allows the data owner to enforce access control on an item-level. And data should remain confidential even against the cloud service provider.

I. INTRODUCTION

More and more companies are implementing item-level tracking in their supply chains using Radio Frequency Identification (RFID) [1] or 2D bar codes. Each RFID tag or bar code carries a unique identifier for each good [2]. Companies are collecting information about the items they handle by scanning the identifier and recording it in their data repositories. Each tuple recorded consists of the item identifier, a timestamp, the location and situation-specific data.

The full benefit of this information can be gained when companies are exchanging their item-level data. Applications, such as anti-counterfeiting [3], supply chain benchmarking [4] or targeted batch recalls [5], are enabled by the shared data. Nevertheless companies are reluctant to share that data [6], [7]. It is unclear what can be inferred from the wealth of information, e.g. strategic relations or best practices. Companies may suffer consequences for unfair behavior. Therefore, fine-grained policies need to be set.

On the one hand, companies want to stay in control over their item-level data and enforce strict access control. On the other hand, the distribution of data causes severe problems in locating and accessing the data [8].

Item-level data is usually partitioned horizontally and tuples corresponding to one item are spread across a number of repositories, e.g. because each company will store the data it gathers in its own repository. Nevertheless, the typical query searches for all tuples corresponding to one item (pedigree). Locating the repositories that contain information about one item is difficult and time-consuming considering the number of repositories and the volume of data. Proposals have been made for discovery servers that contain an index

over all repositories [9]. Nevertheless these proposals neither scale very well, nor do they provide the appropriate level of security.

Considering only the data access performance problem one central repository seems to be the optimal solution. There is no need to locate the repositories and modern database technology can be used to speed up queries. Such a repository could be easily implemented in today's Cloud Computing infrastructure. Nevertheless, this solution does not address the security concerns of the companies. Companies do need to stay in control over their data and should not need to trust a cloud service provider.

In this paper we discuss requirements for an encryption scheme for exchanging item-level data by storing it in a cloud-based data repository.

II. REQUIREMENTS

As already mentioned, we target a scenario with a central repository. Our security requirements for the central repository are

- 1) A party observing the central repository should not be able to track items.
- 2) A party should be able to enforce different levels of fine-grained access control on its items.

The first requirement is important in order to protect against attacks introduced by a central repository. One can imagine an attacker that continuously monitors the central repository and tries to infer as much information as possible. We would like to prevent such an attacker from gaining any information.

The second requirement implies different access control policies. It is a functional requirement on the security mechanism. We anticipate that a data owner has different trust relationships with different parties and he should be able to set the access control policies accordingly. In particular, we want the data owner to be capable of enforcing access control on the following levels:

- A1:** for each tuple
- A2:** for each party, all tuples corresponding to items that the party possessed
- A3:** for each party, all tuples corresponding to items that the data owner previously possessed

These levels are a subset of visibility policies [10] which have been defined for mobile physical objects, such as goods

in a supply chain. The first level A1 allows setting any arbitrary policy on a tuple-level. The second level A2 of access control is particularly useful for item-level tracking. It allows restricting the visibility of items to someone who possessed the item without having to set access control to individual items. One can then engage in fair data sharing agreements with other parties without the risk of disclosing information about other supply chain partners – even by inference. The third level A3 enables including trusted parties, e.g. outsourced manufacturers or service providers. They get full access to the data of their trusting partner.

III. ENCRYPTION SCHEME FOR ITEM-LEVEL DATA

Consider implementing these requirements with traditional cryptography: in both symmetrical and asymmetrical encryption, one key or one key pair would be required for each tuple and for each party. Since an average supply chain produces millions of items with hundreds of supply chain partners, these methods would result in a huge number of cryptographic keys. Furthermore, cryptographic keys would need to be exchanged between parties for each item/tuple produced. Thus, both methods are unpractical.

We follow a different approach: we propose a new cryptographic scheme which only requires a random number for each item, and two cryptographic keys. And it only requires cryptographic keys to be exchanged once, i.e. new items/tuples do not require an exchange of new cryptographic keys. Our cryptographic scheme stores encrypted data in a central repository.

Our cryptographic scheme requires tuples containing two values:

- I : a unique identifier for the combination of one item and one party
- D : encrypted data

Note that I will uniquely identify D , therefore it can be used to query D from the repository.

The challenge of our cryptographic scheme is to on the one hand prevent an observer from inferring information about an item or company from I , but on the other hand let legitimate queries efficiently identify the tuples containing I .

Our cryptographic scheme consists of the following steps in its basic procedure:

- 1) Company i receives or produces an item which is equipped with a unique ID
- 2) Company i collects data about this item, encrypts it, and stores it in the data repository
- 3) Company i sells the item, i.e. it sends it to Company $i+1$
- 4) Later, Company $i+1$ can query and decrypt item-level data that Company i stored in the repository

IV. SUMMARY

In this paper we have discussed requirements for the secure exchange of item-level data along the supply chain using a central repository. According to the requirements, a party with full access to the repository should not be able to infer or forge any information. Furthermore, different levels of fine-grained access control should be enforced, e.g. on each item.

ACKNOWLEDGEMENTS

The work presented in this paper was partly funded by the German government (BMBF) through the *Polytos* project.

REFERENCES

- [1] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*. John Wiley & Sons, Inc., 2003.
- [2] S. Sarma, D. Brock, and D. Engels, “Radio frequency identification and the electronic product code,” in *IEEE Micro* 21(6), 2001.
- [3] F. Kerschbaum and N. Oertel, “Privacy-Preserving Pattern Matching for Anomaly Detection in RFID Anti-Counterfeiting,” in *Proceedings RFIDsec’10*, 2010.
- [4] F. Kerschbaum, N. Oertel, and L. Weiss Ferreira Chaves, “Privacy-Preserving Computation of Benchmarks on Item-Level Data Using RFID,” in *Proceedings ACM WISEC’10*, 2010.
- [5] L. Weiss Ferreira Chaves and F. Kerschbaum, “Industrial Privacy in RFID-based Batch Recalls,” in *Proceedings of InSPEC’08*, 2008.
- [6] M. Eurich, N. Oertel, and R. Boutellier, “The impact of perceived privacy risks on organization’s willingness to share item-level event data across the supply chain,” in *Electronic Commerce Research* 10(3-4), 2010.
- [7] B. Santos and L. Smith, “RFID in the Supply Chain: Panacea or Pandora’s Box?” in *Communications of the ACM* 51(10), 2008.
- [8] B. Fabian, O. Günther, and S. Spiekermann, “Security Analysis of the Object Name Service,” in *Proceedings of the Int. Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing*, 2005.
- [9] S. Beier, T. Grandison, K. Kailing, and R. Rantza, “Discovery Services - Enabling RFID Traceability in EPCglobal Networks,” in *Proceedings of COMAD’06*, 2006.
- [10] F. Kerschbaum, “An Access Control Model for Mobile Physical Objects,” in *Proceedings ACM SACMAT’10*, 2010.