A New Security and Privacy Framework for RFID In Cloud Computing

Süleyman Kardaş*,†, Serkan Çelik*,†, Muhammed Ali Bingöl*,†, and Albert Levi†
*TÜBİTAK BİLGEM UEKAE, Gebze, Kocaeli, Turkey
†Sabancı University, Faculty of Engineering and Natural Sciences,İstanbul, Turkey

***Abstract*—RFID is a leading technology that has been rapidly deployed in several daily life applications such as payment, access control, ticketing, and e-passport, which requires strong security and privacy mechanisms. However, RFID systems commonly have limited computational capacity, poor resources and inefficient data management. Hence there is a demanding urge to address these issues in the light of some mechanism which can make the technology excel. Cloud computing is one of the fastest growing segments of IT industry which can provide a cost effective technology and information solution to handling and using data collected with RFID. As more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Therefore, while integrating RFID into the cloud, the security and privacy of the tag owner must be considered.**

Motivated by this need, we first provide a security and privacy model for RFID technology in the cloud computing. In this model, we first define the capabilities of the adversary and then give the definitions of the security and privacy. After that we propose an example of an RFID authentication protocol in the cloud computing. We prove that the proposal is narrow strong private^{*+} in our privacy model.

***Index Terms*—Cloud Computing, RFID, Security, Privacy**

I. Introduction

Radio Frequency IDentification (RFID) technology has been around for decades. This technology has gained increasing attention as an emerging solution for automatically identifying and/or authenticating remote objects and individuals. RFID based technologies have been rapidly deployed in various daily life applications such as payment, access control, ticketing, and e-passport that require strong security and privacy mechanisms. Security and privacy are two major concerns in these applications. These are definitely critical points when tags are required to provide a proof of identity. The most prominent privacy risk is the tracking of the tag owner, which permits the creation and abuse of circumstantial tag owner profiles. Therefore, an RFID system should provide confidentiality of the tag identity as well as untraceability of the tag owner even the internal state of the tag has been disclosed [15], [18].

Every potential application of RFID systems may require a different approach. As an illustration, manufacturers of consumer goods require a full range of compliance-tagging and verification solutions. When working to meet RFID compliance mandates, today's one foremost exigency is the need to implement a scalable solution that not only satisfies but also allows for future growth. Traditional RFID inventory management solutions are expensive for large amount of items, in the sense that they require self server maintenance and significant IT intervention.

Moreover, for some applications multiple read points may be required to track the products throughout workplace. In conventional systems multiple number of databases can be established which cause several operational problems such that synchronization of the databases, expensive system and difficult and separate management. To realize the benefits of RFID, retailers will need to upgrade their IT infrastructure in a number of areas, and their interfaces with other business will have to be closer. The verification of tagged items by RFID systems provides full traceability from sender (e.g. manufacturer) to receiver by maintaining a single database placed in a cloud computing. This provides assurance that a product has been shipped and delivered.

This is where cloud computing may come in to provide flexibility to access to the database and authenticate the tagged items/persons. A cloud system can be simply thought of as a server farm that has great computational and storage capacity maintained by the some other operators. In fact, this can greatly reduce the start-up costs as well as the drain that can be put on the IT staff for the RFID system maintainer. Thanks to cloud computing, retailers will not need to upgrade their IT infrastructure.

The real value and return on investment of RFIDs come from how the information derived from RFID tags and systems is applied to enterprise applications that control core business processes (inventory management, supply chain management, warehouse tracking, and location control applications). An RFID system using cloud service as a back-end database and computational capacity is strongly relevant when there is multiple facility providers (such as library, sport center, museum etc.) who are connected to a executive enterprise. In addition, centralizing the above RFID applications and integrating them with an executive systems will require a new level of systems integration capabilities. Using a unified cloud database empowers a single authentication system to more effectively manage pricing, events, reduces inventory losses, expands service offerings, and provides entire RFID infrastructures using a single system. The cloud paradigm provides the ability to offer a single card to each user to get service from multiple

applications.

Besides the usability and reach-ability of cloud computing, the main question is to understand and manage the public concern such as the confidentiality and privacy issues. Therefore some skeptic questions may arise. Can we provide the confidentiality and privacy of the user's data in the public cloud domain? Can we maintain an authentication mechanism by using a far distant cloud service like in our private database?

In RFID literature some protocols require exhaustive search on private identity [3], [20] or asymmetric calculation [1], [4], [19], [22] in order to have a strong authentication mechanism. For large systems, these strong private protocols may result in the need of heavy and expensive servers that have fast computational capacity or large storage.

Motivated from the innovations offered by cloud computing, the primary focus of this paper is to propose a security and privacy framework for the existing RFID systems melded with the cloud computing paradigm in order to improve the scalability, boost the performance and maintain the security & privacy of whole systems. We first define the system procedures for our new model. Contrary to the previous models [2], [6], [7], [11]–[14], [21], [23], we have an additional oracle that an adversary can query the cloud system. Then, the adversary classes are described and we give our security and privacy definition. Finally, we propose an efficient RFID authentication as an example for proof of narrow strong privacy according to our model.

The rest of the paper is structured as follows. In Section 2, we first begin with providing a case study for our privacy model. In Section 3, we introduce our novel privacy model which introduces system procedures, adversary oracles and adversary capabilities. Then we describe the security and privacy definitions with respect to the adversary classes. In Section 4, we propose a privacy preserving RFID authentication protocol which is integrated into a cloud computing service and its security and privacy analysis. Finally we conclude the paper with a brief discussion in Section 5.

II. Case Study: Enterprise Cloud Based RFID Technology

In this section, we illustrate how RFID technology can be used to realize in a cloud computing, which provides computation and storage services. This example would help us examine the restrictions of the technologies and the capabilities of adversaries and the challenging issues in RFID application development and deployments.

Let us describe the scenario for our proposed model. Assume that we have an enterprise company that provides several social facilities such as library, museum, sport center and etc that are physically placed in different areas. These facilities are connected to the enterprise through the internet on the cloud service. Each facility has its own access control based on the RFID system that is connected to the cloud computing which owned by the enterprise. In order to benefit from some of these facilities, the clients first buy a membership from the enterprise. The enterprise provides an RFID based membership card to its clients. Then, with the help of this card, a client could authenticate itself to any of these facilities.

In this scenario, all the clients' information are stored in the database of the cloud. Whenever a legitimate client wants to access a facility, the facility will certainly identify and authenticate the person with the help of the cloud. If the authentication protocol used between a user card and a valid reader in a facility does not consider privacy of the clients, the cloud could profile and trace the user. However, for privacy of card owner the cloud should not be able distinguish any users. Besides the design of a secure privacy-preserving RFID authentication protocols rely on an accurate analysis in a formal security and privacy model. For this reason several frameworks have been proposed to formalize security and privacy in the context of RFID system; however, none of them considers this scenario.

III. Our Privacy Model

Our privacy model borrows and extends the concepts from previous models, including virtual tag references, the corruption model that are introduced in [23] and privacy definitions in [13]. Contrary to [13], we consider an RFID system consists of a cloud service, multiple tags, multiple readers where a tag and a reader carry out an identification protocol with the help of the cloud service. Each tag stores a state, the cloud keeps a database of all valid tags, to which tags can be dynamically added by the adversary. Namely, the cloud is the central back-end server which is connected to multiple readers. Adversaries are allowed to interact with all tags and readers and the cloud. In our model, we do not consider the physical characteristics of the radio links as studied by Danev et al. [10] that can be deal with at the hardware level. For privacy, we consider only the contents of the exchanged messages between tags, readers, and the cloud.

In this section, we first present the system procedures and the oracles that an adversary can query. Then, the adversary classes are described. Finally, we give our security and privacy definition.

A. System Procedure

Throughout the paper we modify the common model for RFID systems and use similar the definitions introduced in [8], [23]. An RFID scheme is defined with the following procedures.

- SetupCloud(1^ℓ) : This algorithm first produces a public-private key pair (K_{C_P}, K_{C_S}) for cloud where ℓ is the security parameter, then initializes its database $\mathcal{DB}$.
- SetupReader(1^ℓ) : This algorithm produces a public-private key pair (K_{R_P}, K_{R_S}) for reader where ℓ is the security parameter, then initializes its database $\mathcal{DB}$.

- SETUPTAG$_{K_P}(ID)$: This algorithm generates a tag secret K and the initial state S of a tag with identifier ID. If this tag is legitimate, the pair (ID, K) is inserted into the database.
- IDENT: An interaction protocol between a tag and the reader to complete the authentication transcript.

1) Adversary Oracles: Privacy is defined as a distinguish-ability game (or experiment Exp) between a challenger and an adversary. This game is defined as follows. First of all, the challenger picks a random challenge bit b and then sets up the system S with a security parameter k. Next, the adversary $\mathcal{A}$ can interact with the RFID system by the help of following generic oracles. First of all, $\mathcal{A}$ setups a new tag of identifier ID$_{\mathcal{T}}$. Then, $\mathcal{A}$ can interacts with following two collections of oracles.

Definition 1: (Adversary Oracles-I)

- CREATETAG(ID$_{\mathcal{T}}$) : It creates a free tag $\mathcal{T}$ with a unique identifier ID$_{\mathcal{T}}$ by using **SetupTag**$_{K_{C_P}}$. It also inserts $\mathcal{T}$ into $\mathcal{DB}$.
- LAUNCH()$\rightarrow \pi$: It makes the reader $\mathcal{R}$ start a new $Ident$ protocol transcript π.
- SENDREADER$(m, \pi) \rightarrow m'$: This sends the message m to the reader $\mathcal{R}$ in the protocol transcript π and outputs the response m'.
- SENDCLOUD$(m, \pi) \rightarrow m'$: This sends the message m to the cloud $\mathcal{C}$ in the protocol transcript π and outputs the response m'.
- SENDTAG$(m, vtag)_b \rightarrow m'$: on input vtag, this oracle retrieves the triple $(vtag, \mathcal{T}_i, \mathcal{T}_j)$ from the table D and sends the message m to either $\mathcal{T}_i$ (if $b = 0$) or $\mathcal{T}_j$ (if $b = 1$). It returns the reply from the tag (m'). If the above triple is not found in D, it returns $\perp$.
- DRAWTAG$^b(\mathcal{T}_i, \mathcal{T}_j) \rightarrow vtag$: on input a pair of tag references, this oracle generates a virtual tag reference, as a monotonic counter, $vtag$ and stores the triple $(vtag, \mathcal{T}_i, \mathcal{T}_j)$ in a table D. Depending on the value of b, $vtag$ either refers to $\mathcal{T}_i$ or $\mathcal{T}_j$. If $\mathcal{T}_i$ is already references as the left-side tag in D or $\mathcal{T}_j$ as the right-side tag, then this oracle also returns $\perp$ and adds no entry to D. Otherwise, it returns $vtag$.
- FREE$(vtag)_b$: on input $vtag$, this oracle retrieves the triple $(vtag, \mathcal{T}_i, \mathcal{T}_j)$ from the table D. If $b = 0$, it resets the tag $\mathcal{T}_i$. Otherwise, it resets the tag $\mathcal{T}_j$. Then it removes the entry $(vtag, \mathcal{T}_i, \mathcal{T}_j)$ from D. When a tag is reset, its volatile memory is erased. The non-volatile memory, which contains the state S, is preserved.
- CORRUPT$(T_i) \rightarrow S$: It returns volatile and non-volatile memory of the tag T_i.
- RESULT$(\pi) \rightarrow x$: When π completes, returns $x = 1$ if the tag is identified, $x = 0$ otherwise.

In our model, we also define two another oracles as follows.

Definition 2: (Adversary Oracles-II)

- CORRUPT$(\mathcal{R}_i) \rightarrow S$: It returns volatile and non-volatile memory of the reader $\mathcal{R}_i$.
- CORRUPT$(Cloud) \rightarrow S$: It returns volatile and non-volatile memory of the cloud.

Definition 3: $(Exp_{S,A}())$ By using the DRAWTAG oracle the adversary can arbitrarily select which tags to interact with. Based upon the challenge bit b the system that the challenger presents to the adversary will behave as either the left tags $\mathcal{T}_i$ or the right tags $\mathcal{T}_j$. After A called the oracles, it outputs a guess bit g. The outcome of the game will be $g == b$, i.e., 0 for an incorrect and 1 for a correct guess. The adversary wins the privacy game if it can distinguish correctly the left from the right world being executed.

The advantage of the adversary $Adv_{S,\mathcal{A}}(k)$ is defined as:

$$\left| Pr\left[Exp^0_{S,A}(k) = 1\right] + Pr\left[Exp^1_{S,A}(k) = 1\right] - 1 \right|.$$

2) Privacy Classes: Contrary to previous models proposed in the literature, we consider two types of adversaries such as insider and outsider adversaries. The cloud is expected to be the insider adversary who runs the protocol between a legitimate reader and itself correctly, but might save the messages to distinguish the tags. Namely, the cloud is honest but curious during its protocol runs. However, for the outsider adversaries, similar to Vaudenay privacy class [23], we introduce four privacy classes of polynomial-time bounded adversaries, determined by $\mathcal{A}$'s access to RESULT or CORRUPT oracles. These classes are formally defined as follows.

Definition 4: (Adversary Classes) An adversary $\mathcal{A}$ is a p.p.t. algorithm which has arbitrary number of accesses to either the oracles described in Definition 1 or the oracles described in Definition 2.

- **Insider** $\mathcal{A}$ cannot access to any oracles except CORRUPT(Cloud) oracle described in Definition 2.
- **Weak** $\mathcal{A}$ uses only the oracles given in Definition 1 except CORRUPT(T_i) oracle.
- **Destructive** $\mathcal{A}$ uses only the oracles given in Definition 1 but cannot use any oracle on a tag after using CORRUPT(T_i).
- **Strong** $\mathcal{A}$ uses only the oracles given in Definition 1 without any restrictions.
- **Narrow** $\mathcal{A}$ has no access to RESULT oracle.

We also define X$^+$ and X* privacy notion variants, where X refers to the basic privacy notion. $^+$ refers to the notion that arises when the adversary has also access to CORRUPT$(\mathcal{R})$ oracle. But * refers to the notion that arises when the capabilities of the adversary are further restricted with respect to CORRUPT oracle. The restricted CORRUPT oracle will only return the non-volatile state of the tag but not the volatile memory state. With this restriction, we exclude trivial privacy attacks on multi-pass protocols in which the tags are required to store some information in volatile memory during the session of the protocols.

3) Notion of Security and Privacy:

Definition 5: (Correctness) An RFID scheme is correct if the identification of a legitimate tag only fails with negligible probability with respect to system's security parameter.

Definition 6: (Tag Authentication) An RFID system achieves tag authentication if for every strong adversary and for every tag in the system, the probability of attacker's impersonating any tag is at most negligible. The adversary may interact with the tag they want to impersonate. The adversary can corrupt all tags but not the impersonated tag.

Definition 7: (Privacy [13]). A privacy preserving protocol, modeled by an RFID system $\mathcal{S}$, is said to computationally provide privacy notion X, provided that for all polynomially bounded adversaries $\mathcal{A}$, it holds that $Adv^{X}_{\mathcal{S},\mathcal{A}}(k) \leq \epsilon$, for negligible ϵ.

IV. Our Private Authentication Protocol

A. Preliminaries and Notations

Our proposed protocol is based on Elliptic Curve Cryptography (ECC) and we work on the additive property of ECC . In this paper, the elliptic curve and the generator are selected according to RFC : 5639 document [17]. Points on the curve are represented by capital letters while scalars are represented by lowercase letters.

The $xcoord(.)$ function is the ECDSA conversion function [5], which comes almost for free when using elliptic curves. Assuming an elliptic curve $\mathbb{E}$ with prime order . over $\mathbb{F}_p$, then for a point $Q = q_x, q_y$ with $q_x, q_y \in [0, \ldots, p-1]$, $xcoord(Q)$ maps Q to q_x mod ℓ. We define $xcoord(O) = 0$, where O is the point at infinity. Moreover, $\#E$ represents the number of points on the eliiptic curve.

In this paper, we also use crytographic hash functions which have one-wayness, second preimage resistance and collision resistance property. In our proposed protocol, we treat hash functions as random oracles. Namely, the function $\mathcal{H}$ responds to every query with a truly random response chosen uniformly from $\{0,1\}^{\alpha}$. However, the function always gives the same response for a given input word.

Elliptic Curve Discrete Logarithm. Let P be a generator of a group $\mathbb{G}_\ell$ of order ℓ and let A be a given arbitrary element of G_ℓ The discrete logarithm (DL) problem is to find the unique integer $a \in \mathbb{Z}_\ell$ such that $A = aP$. The DL assumption states that it is computationally hard to solve the DL problem.

B. The Proposed Protocol

In this section, we first give a brief explanation about how to setup the secrets for each party in the RFID system during, then we present the identification protocol.

Let $\mathcal{I}$ be the trusted issuer which setups the system parameters and the secrets of each party. $\mathcal{I}$ first constructs the elliptic curve and selects a generator P. Then $\mathcal{I}$ generates a random private key y for the cloud and computes the corresponding public key $Y = yP$. $\mathcal{I}$ also generates a random unique private key n for each NFC and computes the corresponding public key $N = nP$. For each tag, $\mathcal{I}$ selects a random unique identifier id and also computes the ECDSA signature pair (r, s) on the $ID_x = xcoord(idP)$. Note that, the secrets of the tag are id, r, s, the secret of reader is n, the secret of the cloud is y. On the other hand, the public values of the tag are Y, P, the public values of the reader and the cloud are N, Y, P.

In our proposal, the cloud can distinguish whenever a NFC reader is corrupted or simulated and disallow any interactions from the corrupted reader. The channel between NFC and the cloud is assumed to be secure.

An overview of the proposed protocol is given in Fig. IV-A. First of all, the reader $\mathcal{R}$ generates a random number r_1 which is used for soundness and ensuring privacy. $\mathcal{R}$ computes a point on the elliptic curve with r_1 ($R_1 = r_1P$), then $\mathcal{R}$ sends it to tag $\mathcal{T}$. $\mathcal{T}$ verifies that $R_1 = \mathcal{O}$, the point at infinity and chooses a random number r_2 and calculates $R_2 = r_2P$. Then, $\mathcal{T}$ computes $d_1 = xcoord(r_2R_1)$, $d_2 = xcoord(r_2Y)$, $m_1 = id + r_2 + \mathcal{H}(d_1, d_2, 1)$, $m_2 = r + \mathcal{H}(d_1, d_2, 2)$, and $m_3 = s + \mathcal{H}(d_1, d_2, 3)$ and sends R_2, m_1, m_2, m_3 to the reader. The reader sends R_2 to the cloud. The cloud first checks whether the R_2 is a point on the curve and not a point-at-infinity. If it is a good point then computes $D_2 = y(R_2 + N)$, otherwise sets D_2 with a random point and sends to the reader. After that $\mathcal{R}$ computes $d_1 = xcoord(r_1R_2)$, $d_2 = xcoord(D_2 - nY)$, $ID_x = xcoord((m_1 - \mathcal{H}(d_1, d_2, 1))P - R_2)$,$r = m_2 - \mathcal{H}(d_1, d_2, 2)$ and $s = m_3 - \mathcal{H}(d_1, d_2, 2)$. Finally, the reader checks whether the signature pair (r, s) is the valid signature on ID_x by using ECDSA verification algorithm.

Remark 1: The adversary can never see the cloud server's replays for queried R_2 values. The reason for this claim is, if the adversary does not corrupt the reader, then since NFC and the cloud server have secure channel, the adversary can not observe D_2 values. Moreover, if the adversary corrupts the reader, then due to the detection argument, the cloud server does not return any reply to the adversary.

C. The Security and Privacy Analysis

Theorem 1: The proposed protocol is correct according to Definition 5

Proof: Let T be a valid tag with the identifiers id, r, s, Y and let reader sends R_1 at a protocol run and the tag produces r_2 as a nonce at this protocol run. The correctness of the protocol can be shown by following arguments.

$$
\begin{aligned}
d_1 &= xcoord(r_2R_1) = xcoord(r_1R_2) = d_1 \\
d_2 &= xcoord(D_2 - nY) = xcoord(yR_2 + yN - nY) \\
&= xcoord(r_2Y) = d_2 \\
ID_x &= xcoord((m_1 - \mathcal{H}(d_1, d_2, 1))P - R_2 \\
&= xcoord((id + r_2)P - R_2) = xcoord(idP)
\end{aligned}
$$

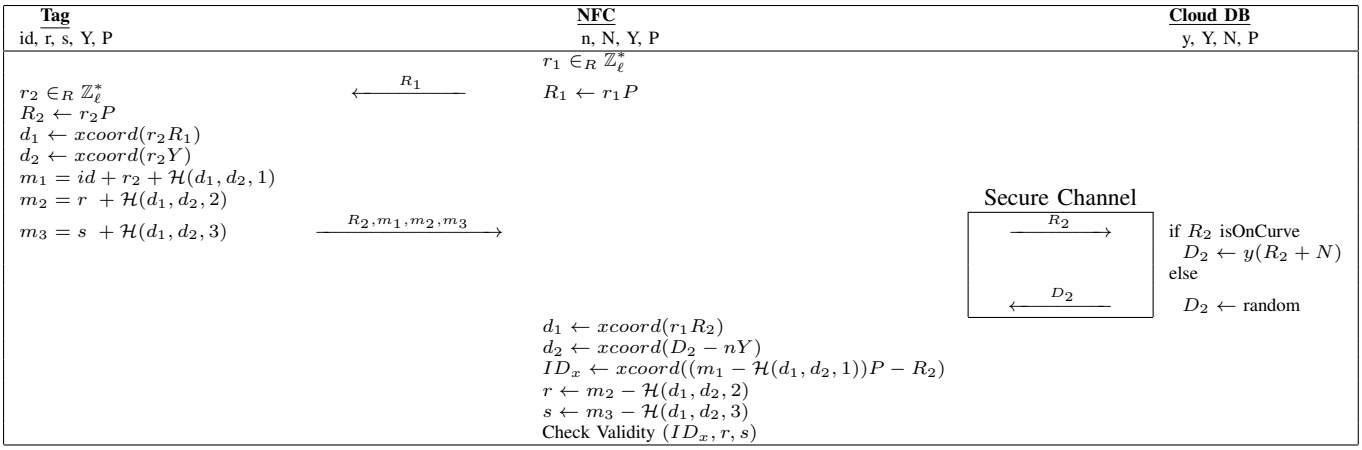

Figure 1. A Narrow Strong Private Authentication Protocol^{+*}.

$$r = m_2 \mathcal{H}(d_1, d_2, 2) = r + \mathcal{H}(d_1, d_2, 2) - \mathcal{H}(d_1, d_2, 2) = r$$
$$s = m_3 \mathcal{H}(d_1, d_2, 3) = r + \mathcal{H}(d_1, d_2, 3) - \mathcal{H}(d_1, d_2, 3) = s.$$

Thus, if a tag is valid, then after a successful protocol run, reader successfully authenticates corresponding tag. ■

Theorem 2: Let $\mathcal{A}$ be a strong adversary$^+$. Then, $\mathcal{A}$ cannot infer the cloud's secret key y from any R_2 and D_2.

Proof: First of all, by Remark 1, the adversary can not have any (R_2, D_2) pair, so for the adversary there is no chance to gain the value of y. However, even the adversary receives the D_2 values for her $SendCloud(R_2)$ queries, she cannot figure out y value. To see that, the following argument can be proposed. Firstly, the adversary should query the points on the curve as cloud sends random points for queried random R_2 points. Since the adversary knows the value of N, for each query she submits, she can calculate $R_2 + N$. Therefore, the adversary has polynomially bounded discrete logarithm problem for elliptic curves. By Remark 1, it is infeasible for the adversary to find the value of y. ■

Theorem 3: Let $\mathcal{A}$ be a strong adversary$^+$. Then, $\mathcal{A}$ cannot steal the all secret values of a tag, id, r, s, if the tag remains uncorrupted.

Proof: First of all, by Remark 1 and the fact that secrets of NFCs are not used in tag side calculations, without loss of generality we can assume that there is only one NFC in the system and the adversary does not apply $Corrupt(Reader)$ oracle. This assumption does not result in loss of the generality as one can regain the advantage loss due to having one NFC for analysis instead of more by running more protocols on the NFC to be used for analysis. Let us fix a tag T and let $W = \{T_0, T_1, \ldots, T_k\}$ be the set of other tags in the system where k is polynomially bounded in l, where l is the security parameter. Let the adversary does not apply the CORRUPT oracle to T and she tries to figure out the secrets of this tag. However, let the adversary can apply any number of CORRUPT oracle to tags in set W. First, may be the most remarkable observation is the adversary does not need to deal with tags in the set W to destroy authentication of the target tag since the tag related secrets are not relevant to other tags' secrets in a deterministic way and if the adversary applies some oracle in the set W, the only useful information for her to get some (r_1, R_1) and (r_2, R_2) pairs. However, the adversary can get the same amount of information by preparing more (r_1, R_1) and (r_2, R_2) pairs beforehand or having more protocol run between the tag and the NFC. Therefore, tag authentication of target tag is not related to the number of tags in the system, but it is related to the number of pairs she prepares beforehand and protocol transactions she can observe or commit with the target tag.

Note that, the adversary has to learn the values of d_1 and d_2 in at least one protocol transaction to get the values of id, r and s. By theorem 2, the adversary can not learn the cloud's secret. Thus, she has to figure out the value of the chosen r_2 value at least one protocol transaction. Therefore, let the adversary create a (r_2, R_2) pairs before starting the attack. Then, let the adversary uses SENDREADER(π) oracle for b times to initiate protocol run between the NFC and the target tag, where a and b are polynomially bounded in l. Note that, the adversary does not need to know the value of r_1, thats why she does not use $SendTag(R_1)$ command for precomputed r_1 values. Therefore, the probability for the adversary to get the value of r_2 at least one protocol transaction is less than

$$(1 - \frac{a}{\#E - b})^b \approx e^{\frac{-ba}{\#E - b}}.$$

Since the values a and b are polynomially bounded in l, then the probability is negligible. ■

Corollary 1: The proposed protocol satisfies tag authentication against strong adversary$^+$.

Proof: This corollary is direct concequence of Theo-

rem 3. ■

Theorem 4: The proposed protocol satisfies narrow-strong^{+*} privacy.

Proof: Let l be a security parameter. First of all, by Remark 1 and the fact that secrets of NFCs are not used in tag side calculations, without loss of generality we can assume that there is only one NFC in the system and the adversary does not apply $Corrupt(Reader)$ oracle. This assumption does not result in loss of the generality as one can regain the advantage loss due to having one NFC for analysis instead of more by running more protocols on the NFC to be used for analysis.

Let A_n be a narrow-strong adversary^{+*} and A_n calls CREATETAG oracle two times and creates the tags T_0, T_1. Then, let the adversary calls the DRAWTAG oracle to have $vtag_1$, which refers either T_0 or T_1 and applies the CORRUPT oracle for both tags to learn the secrets in these tags' non-volatile memory. Note that, it is enough for the adversary to apply CORRUPT oracle only once per tag as their secrets in the non-volatile memories do not change protocol run to protocol run.

Note that, the adversary has to learn the values of d_1 and d_2 in at least one protocol transaction to learn id, r and s values to figure out $vtag_1$ represents which tag. By theorem 2, the adversary can not learn the cloud's secret. Thus, she has to figure out the value of r_2 value at least one protocol transaction. Therefore, let the adversary create a (r_2, R_2) pairs before applying other oracles. After that, the adversary only applies SENDTAG$(vtag_1, R_1)$ oracle for a fixed point R_1 on the curve for p_1 times, where p_1 is polynomially bounded in l. The reason for the adversary only applying one oracle is that different R_1 values has no effect at destroying privacy and applying oracles on reader does not give any advantage to the adversary. Then, the adversaries advantage to destroy the privacy is bounded above by

$$1 - (1 - \frac{a}{\#E - p_1})^{p_1} \approx 1 - e^{\frac{-p_1 a}{\#E - p_1}}.$$

since, p_1 is polynomially bounded in l, the probability stated above is negligible. Thus, creating just two tags is not enough for the adversary.
Now, let the adversary creates two more tags T_2, T_3 and applies DRAWTAG oracle to get $vtag_2$. Similarly, the adversary only uses SENDTAG$(vtag_1, R_1)$ oracle for the same R_1 point for p_2 times, where p_2 is polynomially bounded in l. In this case, the analysis of the adversary's advantage to destroy the privacy for just these two tags T_2 and T_3 is similar to the analysis of the adversary's advantage to destroy the privacy for tags T_0 and T_1. However, the adversary has more tools. If one of the R_2 value returned from $vtag_2$ is equals one of the R_2 value returned from $vtag_1$, then adversary also breaks the privacy. Thus, the total advantage of the adversary is less than

$$2 - (1 - \frac{a}{\#E - (p_1 + p_2)})^{p_1 + p_2} + (1 - \frac{p_1}{\#E})^{p_2}$$
$$\approx 2 - e^{\frac{-(p_1+p_2)a}{\#E-(p_1+p_2)}} - e^{\frac{-(p_1 p_2)}{\#E}}.$$

For the sake of generalization, let the adversary create $2k-4$ more tags and as a total has k $vtag$ reference and let she follows the same steps as described above paragraphs of this proof. Let $M = p_1 + \ldots + p_k$ and $T = \max p_1, \ldots, p_k$, then the total advantage of the adversary is less than

$$\binom{k}{2} + 1 - (1 - \frac{a}{\#E - (M)})^{M} + \binom{k}{2}(1 - \frac{T}{\#E})^{T}$$
$$\approx \binom{k}{2} + 1 - e^{\frac{-Ma}{\#E-M}} - e^{\frac{-(T^2)}{\#E}}.$$

The probability above is negligible as a, M, T are polynomially bounded in l. Thus, the proposed protocol satisfies narrow-strong^{+*} privacy. ■

Theorem 5: The proposed protocol is resistant against insider adversary according to Definition 4.

Proof: According to Definition 4, the insider adversary A_I is only allowed to use CORRUPT(Cloud), so she cannot learn tag related secrets and NFC secrets. Therefore, in terms of insider adversary, the only privacy concern is link-ability. Thus, we play the following game with the adversary. Let there be two tag, T_0 and T_1, the oracle $\mathcal{O}$ chooses $b \in_R \{0, 1\}$, and the tag T_b has p protocol transaction, after that the oracle chooses $b' \in_R \{0, 1\}$ and $T_{b'}$ has k protocol transaction. After that step, the adversary returns 1 if she believes $b == b'$, and returns 1 otherwise. If her guess is correct, she destroys the privacy, otherwise we conclude that the system satisfies privacy against insider attacks.
Let before starting play the game, A_I prepares S (r_1, R_1) pairs and H (r_2, R_2) pairs. Then $\mathcal{O}$ chooses $b \in_R \{0, 1\}$, $b' \in_R \{0, 1\}$, the oracle and the adversary plays the game described above. Before returning the guess, the adversary analyzes the followings: If any of R_1 point or R_2 point in these p transactions is equal to the any of R_1 or R_2 points prepared before the game started by the adversary, then she destroys the privacy, as in each transaction, she knows the value of d_2 and if the above condition satisfied, the she also learns d_1 value of an protocol ran. Thus, she learns the r and s secret of T_b, so she can link this tag's transactions. If this is not the case, similar to the above approach, if any of R_1 point or R_2 point in k transactions with $T_{b'}$ is equal to the any of R_1 or R_2 points prepared before the game started by the adversary, then she destroys the privacy. Moreover, if any of chosen R_1 by NFC in k transactions is equal to any of chosen R_1 by NFC in p transactions, she again destroys the privacy. If any of mentioned analysis does not work, the adversary flips a coin, and returns her guess. Therefore, the

advantage of the adversary is bounded above by

$$\frac{1}{2} + 3 - ((1 - \frac{S}{\#E})(1 - \frac{H}{\#E}))^p + ((1 - \frac{S}{\#E})(1 - \frac{H}{\#E}))^k + (1 - \frac{p}{\#E})^k \approx \frac{1}{2} + 3 - (e^{-\frac{pH+S}{\#E}} + e^{-\frac{kH+S}{\#E}} + e^{-\frac{kp}{\#E}}).$$

Since, S, H, p and k are polynomially bounded in l, then A_I's advantage to destroy the privacy is negligible. Hence, the system is resistant against insider adversaries. ■

D. Performance Considerations

Our proposal requires only one-way hash functions, scalar-ECC point multiplications and the generation of a random number. In order to work on 80-bit security level, the elliptic field size should be at least 160-bits. We can implement our proposal in one of the recent ECC architectures [16], [24]. The architecture [16] for ECC coprocessor needs less than 15 kGE consumes 13, 8 μW of power and takes around 85 ms for one scalar-ECC point multiplication [16]. Wenger and Hutter [24] proposed an ECC coprocessor that only needs 9 kGEs, consumes 32, 3μW of power and requires about 286 ms for one scalar-EC point multiplication. For the implementation of hash functions, in architecture of [9], we need 330 operation clocks for one hash function of 160-bit data and 19.5 μW power consumption at 100 kHz operation clock.

V. Conclusion and Discussion

In this paper, we provide a new security and privacy framework for RFID technology that is integrated into cloud service to leverage the availability and scalability of the system. In this framework, we define the capabilities of the adversary and then give the definitions of the security and privacy. After that we give an example of an RFID authentication protocol in the cloud computing. Using our privacy model analyze the sample protocol and prove that the proposal is narrow-strong private.

References

[1] G. Avoine, "Privacy issues in rfid banknote protection schemes," in *Smart Card Research and Advanced Applications CARDIS*. IFIP, Kluwer Academic Publishers, 2004, pp. 33–48.

[2] ——, "Adversarial model for radio frequency identification," Swiss Federal Institute of Technology (EPFL), Security and Cryptography Laboratory (LASEC, Tech. Rep., 2005.

[3] G. Avoine, E. Dysli, and P. Oechslin, "Reducing time complexity in rfid systems," in *Proceedings of the 12th international conference on Selected Areas in Cryptography*, ser. SAC'05. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 291–306.

[4] M. A. Bingöl, F. Birinci, S. Kardaş, and M. S. Kiraz, "Anonymous RFID Authentication for Cloud Services," *International Journal of Information Security Science*, vol. 1, no. 2, pp. 32–42, June 2012.

[5] D. R. Brown, "Generic groups, collision resistance, and ecdsa," *Des. Codes Cryptography*, vol. 35, no. 1, pp. 119–152, Apr. 2005.

[6] M. Burmester, T. van Le, and B. de Medeiros, "Provably Secure Ubiquitous Systems: Universally Composable RFID Authentication Protocols," in *Securecomm and Workshops, 2006*, 28 2006-sept. 1 2006, pp. 1 –9.

[7] S. Canard, I. Coisel, J. Etrog, and M. Girault, "Privacy-preserving rfid systems: Model and constructions," 2010. [Online]. Available: http://eprint.iacr.org/2010/405

[8] ——, "Privacy-Preserving RFID Systems: Model and Constructions," Cryptology ePrint Archive, Report 2010/405, IACR, 2010.

[9] Y. Choi, M. Kim, T. Kim, and H. Kim, "Low power implementation of sha-1 algorithm for rfid system," in *Consumer Electronics, 2006. ISCE '06. 2006 IEEE Tenth International Symposium on*, 0-0 2006, pp. 1 –5.

[10] B. Danev, T. S. Heydt-Benjamin, and S. Čapkun, "Physical-layer identification of RFID devices," in *Proceedings of the 18th conference on USENIX security symposium*, ser. SSYM'09. Berkeley, CA, USA: USENIX Association, 2009, pp. 199–214.

[11] R. H. Deng, Y. Li, M. Yung, and Y. Zhao, "A new framework for rfid privacy," in *Proceedings of the 15th European conference on Research in computer security*, ser. ESORICS'10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 1–18.

[12] J. Ha, S. Moon, J. Zhou, and J. Ha, "A new formal proof model for rfid location privacy," in *Proceedings of the 13th European Symposium on Research in Computer Security: Computer Security*, ser. ESORICS '08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 267–281.

[13] J. Hermans, A. Pashalidis, F. Vercauteren, and B. Preneel, "A new rfid privacy model," in *Proceedings of the 16th European conference on Research in computer security*, ser. ESORICS'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 568–587.

[14] A. Juels and S. A. Weis, "Defining strong privacy for rfid," *ACM Trans. Inf. Syst. Secur.*, vol. 13, pp. 7:1–7:23, November 2009.

[15] S. Kardaş, S. Çelik, M. Yildiz, and A. Levi, "PUF-enhanced offline RFID security and privacy," *Journal of Network and Computer Applications*, vol. 11, no. 12, pp. 1–11, 2012.

[16] Y. K. Lee, L. Batina, D. Singelée, and I. Verbauwhede, "Low-cost untraceable authentication protocols for rfid," in *Proceedings of the third ACM conference on Wireless network security*, ser. WiSec '10. New York, NY, USA: ACM, 2010, pp. 55–64.

[17] M. Lochter and J. Merkle, "Elliptic curve cryptography (ecc) brainpool standard curves and curve generation," 2010.

[18] A.-R. Sadeghi, I. Visconti, and C. Wachsmann, "PUF-Enhanced RFID Security and Privacy," in *Secure Component and System Identification – SECSI'10*, Cologne, Germany, April 2010.

[19] G. Shen and B. Liu, "Research on embedding ecc into rfid authentication protocol," *IEEE TrustCom/IEEE ICESS/FCST, International Joint Conference of*, vol. 0, pp. 1835–1838, 2012.

[20] B. Song and C. J. Mitchell, "Rfid authentication protocol for low-cost tags," in *Proceedings of the first ACM conference on Wireless network security*, ser. WiSec '08. New York, NY, USA: ACM, 2008, pp. 140–147.

[21] T. Van Deursen, S. Mauw, and S. Radomirović, "Untraceability of rfid protocols," in *Proceedings of the 2nd IFIP WG 11.2 international conference on Information security theory and practices: smart devices, convergence and next generation networks*, ser. WISTP'08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 1–15.

[22] S. Vaudenay, "Rfid privacy based on public-key cryptography," in *ICISC 2006. LNCS*. Springer, 2006, pp. 1–6.

[23] ——, "On privacy models for rfid," in *Proceedings of the Advances in Crypotology 13th international conference on Theory and application of cryptology and information security*, ser. ASIACRYPT'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 68–87.

[24] E. Wenger and M. Hutter, "A hardware processor supporting elliptic curve cryptography for less than 9 kges," in *Proceedings of the 10th IFIP WG 8.8/11.2 international conference on Smart Card Research and Advanced Applications*, ser. CARDIS'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 182–198.