VOL. 11, NO. 7, APRIL 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

A NOVEL CONCEPT OF SECURITY AUTHENTICATION AS A SERVICE TO ENHANCE RFID BASED MANUFACTURING

Irfan Syamsuddin
CAIR - Center for Applied ICT Research, Department of Computer and Networking Engineering, State Polytechnic of Ujung Pandang, Makassar, Indonesia
E-Mail: irfans@poliupg.ac.id

ABSTRACT

RFID plays a significant role in current manufacturing automation. Automatic identification as fundamental characteristic of RFID enables manufactures to reduce cost and time which in turn let them increase total productivity. However, security is still regarded as a serious issue to entirely deploying RFID for whole identification processes of manufacturing systems. This paper proposes a new insight on how to tackle the security problem by taking into account cloud computing technology to current RFID based manufacturing system. After careful review on related literature, hash chain authentication protocols in different approaches were chosen as the viable option to address the problem. Using cloud computing paradigm, a novel cloud based RFID manufacturing system powered by hash chain authentication protocol is conceptualized from the perspective of Security Authentication as a Service.

Keywords: cloud manufacture, RFID authentication protocol, hash chain, security as a service.

INTRODUCTION

Radio frequency identifications (RFID) have been seen in a variety of applications. The proliferation of RFID tags and readers also introduces a number of new ways of business applications such as objects identification in industries.

Adoption of RFID technology in the manufacturing industry is mainly due to the ability of RFID to perform identification mechanism simpler and faster as well as easier in comparison to other technologies previously. These features significantly improve the performance of the identification process which is strongly required by the manufacturing automation.

RFID systems consist of tags and readers. While tags operate as transponders, readers act as transceivers. In case of more complex applications, a database server is required to store information comes from both transponders and receivers sides (Syamsuddin, *et al*, 2008).

The process of RFID communication started when RFID reader request access to the RFID tag and return the reply to the database server. After identification and authentication processes on server side, then server will return the information of RFID tag to the reader (Syamsuddin, *et al,* 2008) (Han, *et al,* 2007).

RFID's ability to provide better results in improving business efficiency in terms of time and cost, implementations of RFID in manufacturing have been growing in the last decade. In developing countries such as Indonesia, industries already realized that RFID offers simplicity for object identification and communication which is needed in todays large warehouses. It is believed that RFID will continue to play a significant role for future manufacturing systems as automatic identification is the core characteristic of RFID which eventually improve profit and reduce cost (Wang, *et al*, 2010).

However, security and privacy are two main barriers to prevent RFID adoption. Since communication between RFID tag and the readers is wireless based, any common attacks to wireless communications also affect RFID.

The issue will be tackled by proposing a new cloud based RFID authentication system to support secure manufacturing system using Software as a Service model. Therefore, this paper is organized as follows. Related RFID authentication protocols, particularly those applying hash chain based are widely desvribed and presented in section 2. In the next section, a new concept of Cloud RFID Manufacturing is described and argued. Finally, conclusion and future research direction is presented in the last section.

RFID Authentication protocols

Taking into account inherent limitations of RFID's wireless communications, authentication protocols are introduced and tested by researchers. As RFID tag is very limited in size, it is a big challange to equip it with secure algorithms since more complex one will be out of its capacity (Han, *et al*, 2007).

Hash chain algorithm is a cryptography approach for safeguarding against password and eavesdropping by applying a one-way hash function h(.) recursively to an initial seed value s which then creates a hash chain of length N.

$$hN(s) = h(h(...h(s)...)) \text{ (N times)}$$

The last element hN(s) is also called the tip T of the hash chain. By knowing hN(s), hN-1(s) could not be generated by those who do not know the value s, however given hN-1(s) its correctness can be verified using hN(s).

This property of hash chains has evolved from the property of one-way hash functions (Wang, *et al*, 2010) (Lamport, 1981).

The advantage of hash chain approach lies mainly on its simplicity and relatively strong security mechanism which has produced a number of hash chain RFID authentication protocols. Syamsuddin,et.al (2008) has described ten common protocols of RFID authentication based on hash chain approach.

The first one is that proposed by Ohkubo *et al*. (2003) which is often cited as the earliest approach in suggesting hash chain algorithm to be applied in RFID protocol. The basic concept is refreshing the identifier of the tag each time it is queried by a reader. Then RFID identities are changed on each read based on hash chains in two ways communication of RFID tag.

Hash Lock, another hash chain based algorithm proposed by Weis et al.(2004) is a RFID protocol which uses a simple cryptographical controller to access protocol for RFID tag by using hash locks approach. By doing so, only authorized ones would be able to look up the tags key in a database of key-hash pairs.

Other approach is a Hash-Tree based authentication protocol for RFID tags (2004). This protocol utilizes a dynamic amount of computation required per tag, which depends on the number of tags available in the hash-tree which makes it secure enough to anonymity attack.

In other paper, Henrici and Muller (2004) exemplifies how a new hash function in the tag and data management at the back-end could offer a high degree of location privacy and is resistant to many forms of attacks. Using the protocol, for RFID taq only requires a single message exchange, although the communications channel is not be reliable and the reader/third parties are not trusted.

Similarly, a new protocol to prevent RFID from replay attack is explained by Avoine and Oechslin (2005). This is basically a modification of previous protocol (Henrici and Muller, 2004) by combining three layers of RFID system, namely application, communication and physical.

Different hash chain algorithm called Anonymous Mutual Authentication RFID protocol is introduced by Dimitriou (2005). The objective of this protocol is to protecting forward privacy from cloning and privacy attacks by creating secret key shared between tag and database, and then refreshed to avoid tag tracing.

Hash-Based Challenge-Response is the following protocol presented by Rhee *et al.* (2005). It is aimed at providing security protection mechanism from the replay and spoofing attacks. The proposed protocol is based on challenge response using one-way hash function and random number which is claimed suitable for security database environment. Hash chain function is used in the protocol to guarantee secret key in the form of ID. Then, the tag does not need to update the secret key which avoids attacks by interrupting the session. However, this solution does not provide forward secrecy which means if a tag can be compromised then attacker will be able to trace the past communications from the same tag.

Lee *et al.* (2005) proposed a new RFID authentication protocol with hash chain. The objective of this effort is to solve the desynchronization problem by maintaining a previous identification number in the database server. However, since the hashed identification number is always identical, an adversary who queries tag actively without updating identity able to trace the RFID tag.

Likewise, RFID authentication scheme with a hash function and synchronized secret information was introduced by Lee, *et al*. (2006). The protocol is aimed at securing user privacy including against tag cloning attack through an additional hash operation. Unfortunately, this protocol suffers from desynchronization attacks that could be conducted by adversaries. This occurs due to unavailability of PRNG in the RFID tag while the server does not know how many times an RFID tag may have not yet updated its secret information.

Finally, Han, *et al*. (2007) offer new kind of mutual authentication protocol to solve some problems of previous protocols. In their protocol, the authentication mechanism is supported by a monitoring component. The component which exists in database server constantly monitors the synchronized secret information between RFID tag and reader. This protocol is argued to provide more secure communication mechanism since the communication between tag, reader and database is mutually authenticated and constantly monitored.

Table-1. Security assessments of hash chain protocols.

Algorithm	Privacy	Anonymity
[5]	Yes	Yes
[6]	Yes	Yes
[7]	No	Yes
[8]	Yes	Yes
[9]	Yes	Yes
[10]	Yes	Yes
[11]	Yes	Yes
[12]	Yes	Yes
[13]	Yes	Yes
[14]	Yes	Yes

Comparative study on these specific RFID hash chain protocols in terms of its security properties (privacy and anonymity) could be seen in review papers such as by Syamsuddin, *et al.* (2008) and Syamsuddin (2013) as summarized in table 1.

Secure Cloud RFID manufacturing

The term of Cloud Manufacturing (CM) refers to a new manufacturing paradigm developed from existing advanced manufacturing models and enterprise information technologies under the support of cloud computing, Internet of Things (IoT), virtualization and service-oriented technologies, and advanced computing technologies (Günther, 2008).

In addition, Cloud RFID Manufacturing is an extended model of CM which utilizes Cloud computing (third party) for particular services, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS) instead of deploying it independently.

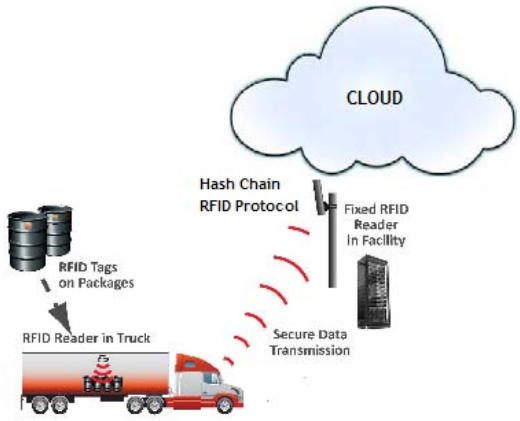

Figure-1. Cloud RFID Manufacturing System.

In this study, the Cloud RFID Manufacturing as depicted in Figure-1 will be improved in terms of its security and privacy by deploying hash chain algorithm to its RFID authentication protocol. The hash chain RFID protocol is an extended model for Cloud Manufacturing which utilizes Cloud computing (third party) for particular services, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS) instead of deploying it independently.

While industries with RFID based automation in their manufacturing need to keep profitable to stay in business, they also consider their assets as important thing to protect. Efforts to make reasonable decision in balancing between business profit of manufacturing processes and urgent need to protect sensitive data is the main challenge for these enterprises that always consider lowest investment with maximum return.

Improving the security and privacy of Cloud RFID Manufacturing while keeping investment cost as lower as possible might be performed by deploying hash chain RFID authentication protocol as Security as a Service. SecaaS offers a way for enterprises to access security services that are robust, scalable and cost effective such as hash chain RFID protocol.

Cloud security as a service works by handling protocol for secure RFID privacy protection scheme is described as follows (Ohkubo, *et al*, 2003).

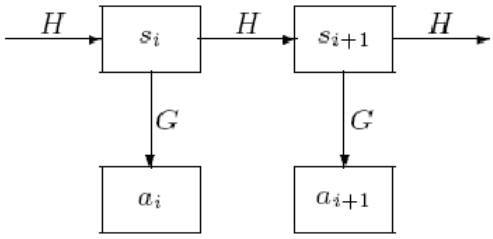

Figure-2. Hash chain in RFID application.

Authentication process of RFID protocol employs different hash chain techniques which can be requested by user. In this case any users that require to deploy secure RFID based manufacturing system. It is employed to renew the secret information contained in the tag from *G* to *H*. After a tag has initial information *s1*, then in the *i-th* transaction with the reader, the RFID tag will sends answer *ai* = *G(si)* to the reader, and followed by renewing secret *si*+1 = *H(si)* as determined from previous secret *si*,

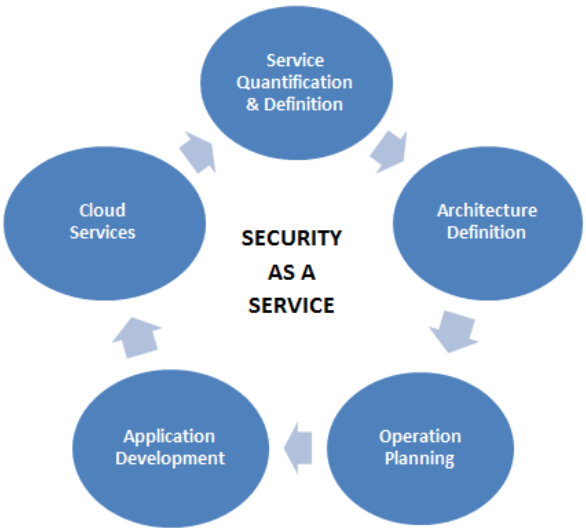

Figure-3. Development lifecycle of SecaaS for RFID Manufacturing System.

A novel concept of Secure Cloud RFID Manufacturing based on Hash Chain RFID Protocol might be deployed in five stages as presented in figure 3. It starts with service definition, architecture definition, operation planning, application development and finally running a novel RFID authentication protocol as cloud services (Syamsuddin and Al-Dabass, 2014) which offers flexibility for users to apply it only whenever required.

CONCLUSIONS

A novel concept of delivering RFID authentication protocol based on hash chain has been presented and illustrated in the form of Security Authentication as a Service. A number of hash chain algorithms are selected to be applied as cloud security services for user whenever they need it in pay as you go basis. This approach is considered as a best solution for industry to enhance its security in cloud environment.

In the future, the research will be enhanced by running the algorithm in cloud simulation environment in order to find out level of adaptivity according to different user's requirements as well as the most efficient RFID protocol to deploy.

ACKNOWLEDGEMENT

This research received funding from Ministry of Research and Higher Education, Republic of Indonesia under the scheme of International Research Collaboration and Publication Research Grant year 2015.

REFERENCES

I Syamsuddin, T.Dillon, E.Chang and S.Han. 2008. A survey of RFID authentication protocols based on hash-chain method. Convergence and Hybrid Information Technology, 2008. IEEE-ICCIT'08. Third International Conference on. 2: 559-564.

I Syamsuddin, 2013. State of The Art on Secure and Low Cost RFID Authentication Protocols for RFID based Vehicle License Plate, International Journal on Smart Sensing and Intelligent Systems, 6(5): 1949 – 1969

S. Han, T.S. Dhillon and E. Chang. 2007. Anonymous Mutual Authentication Protocol for RFID Tag Without Back-End Database, MSN 2007, LNCS 4864. pp. 623-632.

Y.M.Wang, Y.S.Wang, and Y.F.Yang. 2010. Understanding the determinants of RFID adoption in the manufacturing industry. Technological Forecasting and Social Change. 77(5): 803-815.

Lamport, 1981, Password Authentication with Insecure Communication, Communications of the ACM. 24(11): 770-772.

M. Ohkubo, K. Suzuki and S. Kinoshita. 2003. Cryptographic approach to privacy-friendly tags, RFID Privacy Workshop.

S.A. Weis, S.E. Sarma, R.L. Rivest, D.W. Engels. 2004. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, Security in Pervasive Computing. LNCS no. 2802, pp. 201-212.

D, Molnar and D. Wagner. 2004. Privacy and Security in Library RFID Issues, Practices, and Architectures, in ACM Conference on Computer and Communication Security.

D, Henrici and P. Muller. 2004. Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers. In: Proceedings of Workshop on Pervasive Computing and Communications Security.

G. Avoine and P. Oechslin. 2005. RFID Traceability: A Multilayer Problem, Financial Cryptography.

T. Dimitriou. 2005. A Lightweight RFID Protocol to Protect against Traceability and Cloning Attacks. In: International Conference on Security and Privacy for Emerging Areas in Communication Networks, September.

K. Rhee, J. Kwak, S. Kim and D. Won. 2005. Challenge-response based RFID authentication protocol for distributed database environment. International Conference on Security in Pervasive Computing, SPC. pp. 70-84.

S.M. Lee, Y.J. Hwang, D.H.Lee and J.I.Lim. 2005. Efficient Authentication for Low-Cost RFID Systems. In: International Conference on Computational Science and Its Applications. pp. 619-627.

S. Lee, H. Lee, T. Asano and K. Kim. 2006. Enhanced RFID Mutual Authentication Scheme based on Synchronized Secret Information, AUTO-ID Labs White Paper.

S. Han, V. Potdar and E. Chang. 2007. Mutual Authentication Protocol for RFID Tags Based on Synchronized Secret Information with Monitor. ICCSA 2007, LNCS 4707, pp. 227-238.

I Syamsuddin and D. Al-Dabass, 2014. Selection of IPv6 Attributes for Efficient Cloud Computing Development Towards Green E-Government in Indonesia,.International Journal of Simulation--Systems, Science & Technology 15 (2): 85-90

O.P.Günther W.Kletti and U.Kubach. 2008. RFID in Manufacturing. Springer Science and Business Media.