ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 2, Issue 4, April 2013

Efficient RFID Authentication in Cloud Computing

Sherin Jobe, Venifa Mini.G and Jeya A.Celin J.

Abstract— Cloud computing is one of the fastest growing segments of IT industry since the users commitments for investment and costs are in relation to usage. Social networks in cloud are used to reflect real world relationships that allow users to share information and form connections between one another, essentially creating dynamic Virtual Organizations. Anonymous authentication is a technique enabling users to prove they have privilege without disclosing real identities. Many existing anonymous authentication protocols assume absolute trust to the cloud provider where all private keys are stored. This trust result in serious security and privacy issues in cloud provider. In the proposed work secure and efficient anonymous mutual authentication protocols using Radio Frequency Identification technology for cloud services are implemented based on ZKP technique. Zero Knowledge Proof is an interactive system where one party wants to prove its identity to a second party using a password but does not want the second party to learn anything about the password. Finally present experimental results and validate the acceptable performance impact of our deployment on a modern social network.

Keywords— Authentication, RFID, ZKP.

I. INTRODUCTION

Social networks provide a platform to facilitate communication and sharing between users, therefore modeling real world relationships. The structure of a Social Network is essentially a dynamic virtual organization with trust relationships between friends .A Social Cloud is a scalable computing model in which virtualized resources contributed by users are dynamically provisioned among a group of friends. Compensation for use is optional as users may wish to share resources without payment. Access to a cloud discloses a user's real identity; the user could still be unwilling to accept this issue. Thus, the user authentication without identifying the real identity, called anonymous authentication is required. In order to preserve user privacy and allow anonymous authentication/access in a cloud, users can anonymously authenticate themselves as part of authorized users/groups to the cloud provider. Users can anonymously access and modify resources. The authentication between the user and the service can be achieved via Radio Frequency Identification (RFID), which is a means for identifying objects via a radio signal, and enables automated data gathering in a variety of applications. A typical RFID system is setup by a set of readers, a number of RFID tags and a backend server. In general sense, an RFID tag is known as a small integrated circuit with a unique identifier which transmits data over the air in response to interrogation by an RFID reader. In this paper the RFID tag authentication is set up for modern social networking sites where users can share content with their friends and can develop social ties among each other. Users have to login using RFID tag with their corresponding one time identifier PIN, user name and password.

Zero Knowledge Password Authentication Protocol (ZK-PAP) in which the user can authenticate himself to the server without revealing the password. The protocol uses a challenge-response mechanism (between the server and client) based on nonce. A nonce is a randomly generated number to be used only once throughout the session in order to avoid replay attacks. Only authorized users can access the shared services such as videos, text messages, mp3files etc. A mandatory access control mechanism in order to enforce confidentiality and integrity between a large numbers of users. This mechanism works like a naturally pre distributed secret information. A user selects a set of questions and its corresponding answers. Whenever a new user wants to join in the existing group should answer for the questions. If there are more similarities then the user can join in the group or else rejected.

II. LITERATURE REVIEW

The existing authentication techniques mainly focus on the device authentication. Since the web browser is connected to cloud there will be more authentication challenges. Thus a more user centric approach should be developed with more security. These are the papers reviewed for the work. The authors of [1] extend their work to provide protocols for two-party secure roaming system. This may provide either weak or strong anonymity, becoming more complex if strong anonymity is required, this is essentially device-level authentication and a user cannot establish and authenticate their credentials on a separate device. A similar problem for mobile networks is tackled in [2] but in this work the focus is primarily on use of efficient key exchanges to ensure that a mobile terminal is not exposed to eavesdropper or DoS attacks. The resulting protocol is also more efficient and some of the techniques employed in this work are closely related to our own, however this research is again directed to device authentication, rather than user-level authentication. Building control networks are particularly vulnerable from a security perspective as, in contrast to mobile networks, they are designed for a closed community [3]. Similar arguments have applied to home networks, but as such networks link into cloud services more attention needs to be paid to enhanced authentication of users. In [4] the authors implement a mutual authentication protocol using nested one-time secret mechanisms. Such an approach could have value in the context of certain pre-paid network services, but again we

Manuscript received March, 2013.

Sherin Jobe B.E,doing M.E.degree in Computer Science &Engineering ,Noorul Islam University,Tamilnadu,India, (Phone:08943751601,
Venifa Mini.G B.E.,M.E.,doing Ph.D.
J.Jeya.A.Celin.B.Sc,M.C.A,Ph.D

find a relatively complex protocol making it less attractive for CE applications. A key drawback of the authentication protocols described in the previous section is that they all rely on the use of cryptographic keys generated within a specific device. Thus they represent device-level authentication. For mobile wireless services where each user is linked to the network via a unique device this is quite acceptable and even a desirable approach. However access to a home network could be over a range of devices, via: smart-phone, tablet, laptop computer, remote control or wall-panel. But following today's rapid evolution in mobile and cloud services users now expect to gain access to their personal environment in a uniform manner and thus we need to authenticate the user rather than the device. Lin and Lai [5] described a flexible authentication scheme using a biometric smart-card to read fingerprints combined with a changeable user password. Today, with embedded facial analysis algorithms in our camera-phones and more sophisticated system-on-chip (SoC) technologies it is clear that device-level biometric authentication is feasible. Several researchers have remarked on the potential to use biometrics for content or service encoding in addition to basic authentication [6, 7 ,8] and [9].In[10] a one-time password using smartcards for home networks with device level authentication. The scheme uses lightweight computation modules including hashed one time password and hash chaining technique along with low cost smart card technology. A robust and efficient user authentication scheme uses HOTP algorithm and hash chaining technique. HOTP is an HMAC event-based one-time password. . To create a one-time password (OTP), a user will enter their PIN into the security token and generate an OTP to validate the requested transaction. Face recognition [7] is used to determine if the authenticated user continues to view the content and the display will eventually time-out if they leave the room or turn away from the display. Peer-to-peer networking creates a relational framework on top of the existing TCP/IP infrastructure of the Internet. In addition to the ability to exchange raw data, it is also possible to build higher-level functionality on top of such networks. Most people are now aware of the rapid development of peer-to-peer social networks and popular applications based on these networks such as Facebook. Interestingly the concept of social networks extends back before their introduction on the Internet [11]. Mirroring the characteristics of human social networks the concepts of reputation and trust have been rediscovered in online communities [12] and form the basis for many emerging social-networking technologies and next-generation computer applications. An example of these technologies is D-FOAF [13]. It provided a distributed trust component for using social networks as data sources. In [14] outlines vision of creating a Social Storage Cloud, looking specifically at possible market mechanisms that could be used to create a dynamic Cloud infrastructure in a Social network environment.The authors in [15] propose an authentication scheme for mobile users of cloud services that is based on a behavioral authentication approach. The authors of [16] outline the RFID authentication using threshold cryptosystem critically relies on tag corruption, no internal state mechanism is given, and no mutual authentication is performed. The ZKP privacy is stronger than Ind privacy [17].The Ind privacy is not precisely specified the time point of tag corruption The unp privacy [18] based on unpredictability of the protocol output.Unp privacy excludes the use of public key encryption in RFID protocols.

III. SYSTEM ARCHITECTURE

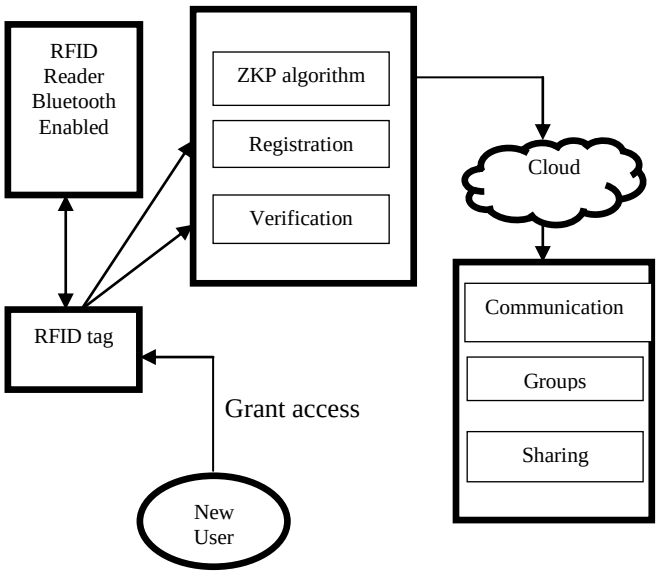


Fig1: Architecture of RFID authentication in cloud

Fig1.shows the architecture of RFID authentication on social network in cloud. The RFID tag is interrogated with the RFID reader and the corresponding PIN number is scanned. The username and password is generated and should be private to the tag owner. Privacy is achieved by zero knowledge proof protocol where the attacker can't determine which tag is accessing and can't get any information about the tag's owner. The authenticated tag owner can be connected to the cloud social network. When a new user wants to join in the tag owners group only authorized users with more similarities with the owner can be permitted.

IV AUTHENTICATION

Now a days cloud computing is facing challenging authentication issues. Most user-facing services today still use simple username and password type of knowledge-based authentication, Thus the most effective way to ensure users are adequately authenticated when using browsers to access services in the cloud, is to facilitate an additional authentication factor outside of the browser in addition to username/password essentially multi-factor authentication In our proposed work an efficient multifactor authentication using RFID tags are implemented.

A. RFID system

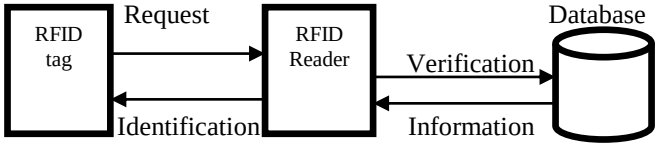


Fig2: Architecture of RFID system
s

RFID tags are low-cost electronic devices, from which the stored information can be collected by an RFID reader efficiently at a distance without the line of sight. RFID system consists of three components:

Tags, consist of an integrated circuit with a small antenna. Each tag will send its identifier (ID) when interrogated.

Reader communicate with a database and with the tags. They are responsible of performing the queries to the tags.

Database with information of the tags

B. Performance of RFID scheme

RFID schemes cannot use computationally intensive cryptographic algorithms for privacy and security because tight tag cost requirements make tag side resources (such as processing power and storage) scarce.

• Capacity minimization: The volume of data stored in a tag should be minimized because of the limited size of tag memory.

• Computation minimization: Tag-side computations should be minimized because of the very limited power available to a tag.

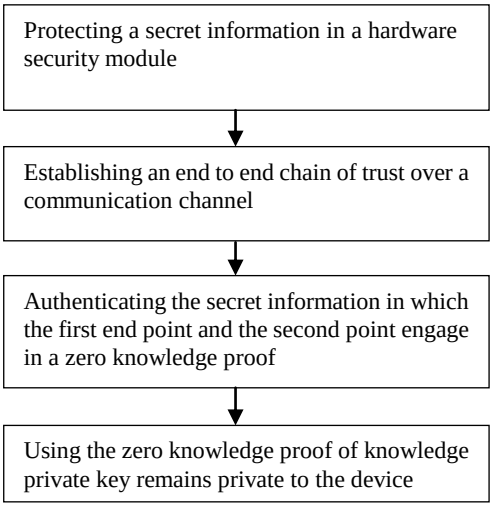
• Communication compression: The volume of data that each tag can transmit per second is limited by the bandwidth available for RFID tags

• Scalability: The server should be able to handle growing amounts of work in a large tag population. It should be able to identify multiple tags using the same radio channel Performing an exhaustive search to identify individual tags could be difficult when the tag population is large

C. Zero knowledge proof

Zero knowledge proofs (ZKP) are proofs that show a statement to be valid without revealing anything except the veracity of the statement to be proven. With the rise in ubiquitous computing, we are using mobile phones for daily tasks. There is a need to preserve the privacy and not reveal information that can be abused by hackers. Zero knowledge proof can be used when someone needs to prove the possession of critical data without revealing the actual data. Zero Knowledge Proof is two types interactive proof and non-interactive proof.RFID tag authentication is based on non-interactive proof. Zero knowledge proof privacy in RFID tag concerns regarding an attacker can't determine which tag he is accessing and can't get any information about the tag's owner.RFID tag ID and PIN will be private to the tag owner.The secret information in the tag is always kept secret and mutual authentication takes place between the reader to the tag and the tag to the reader.

D. Hardware Based Zero Knowledge Authentication



E. RFID tag authentication based on ZKP

Registration phase

Tag Ti wants to register in remote server S.Tag chooses its PIN, ID and Password.

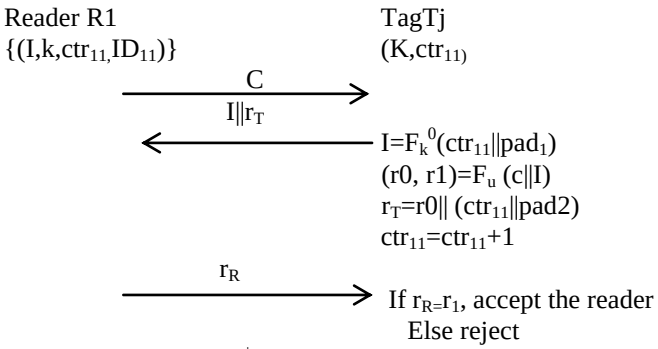
Login phase

This phase provides a secure login with the tag which is achieved by zero knowledge password authentications.

Verification phase

RFID system settings consists of a reader R1 and a set of t tags=$\{T1\ldots..T_t\}$,t is a polynomial in security parameter k.The reader and the tags are probabilistic polynomial time Turing machines[17],the reader secret key K_R and initial internal state S_R^0,the database DB^0 for R1.ZKP privacy has blind access to tags. Let $A^S(R1,T^l,I^l(T_c),aux^l)$ be a PPT algorithm.S={S1,S2,S3,S4} queries. A has blind access to challenge tag $T_c \varepsilon T^l$ if A interacts with T_c via a special interface I^l.To send a message m to T_c,A sends to I^l a special S2 query of the form sendT(challenge,m) after receiving S2 query I^l invokes T_c with sendT(T_c,m) and returns to A the output by T_c. From the view point of A it does not know which tag it is interacting with. Let $F_k:\{0,1\}^{2k} \rightarrow \{0,1\}^{2k}$ be a pre specified PRF[17],k is a security parameter. When a tag T_j with identity ID_{11} registers to reader R,it is assigned a secret key $k\varepsilon R\{0,1\}^k$,a counter ctr_{11} of length l_{ctr11} with initial value 1.R computes the initial index as $I=F_k^l(1\|pad1)$ and so on and stores the tuple (I,ctr_{11},K,ID_{11}) into the database. Only valid tag is accepted or else rejected. The proposed RFID privacy satisfies adaptive completeness and mutual authentication. The protocol (R1, T1) satisfies adaptive completeness such that after desynchronization attacks made by the adversary the execution between reader R1 and the tag T1 is complete. Mutual authentication is satisfied such that reader to tag authentication and tag to reader authentication. No corrupted tag interferes in the tag to reader communication. Only clean tags that are not corrupted can be read by the reader efficiently. The zkp privacy in RFID tag avoids replay attacks. The zkp privacy achieves forward and backward privacy, if the adversary interprets during the ongoing session it will not get any information about the reader.

F.RFID Protocol



If find a tuple (I,k,ctr_{11}^l,ID_{11}), then
Compute $(r0, r1) = F_k(c\|I)$
If $ctr_{11}^l\|pad_2 = r0\|r_T$, then
Accept the tag, send back $r_R=r_1$
Update $ctr_{11}^l=ctr_{11}^l+1$ and $I=F_k^0(ctr_{11}^l\|pad_1)$
Else if $(I^l,k,ctr_{11}^l,ID_{11})$
Accept the tag
Update $ctr_{11}^l=ctr_{11}+1$ and $I^l=F_k^0(ctr_{11}^l\|pad_1)$

Else reject

V IMPLEMENTATION

To enable portability between devices the RFID tag authentication in social network is implemented in Dotnet.The implementation was tested on mantis™-series 303MHZ tag and mantis™ reader manufactured by RF code.fig4 shows the screen shots of RFID tag authentication in a social network.

Fig: 4 RFID tag authentication

Click the Add New Tag button, fig5 shows dialog window asking for the RFID tag ID, username, and password

Fig: 5 Update tag

Fig6 depicts the computation performance of RFID authentication with existing authentication techniques.

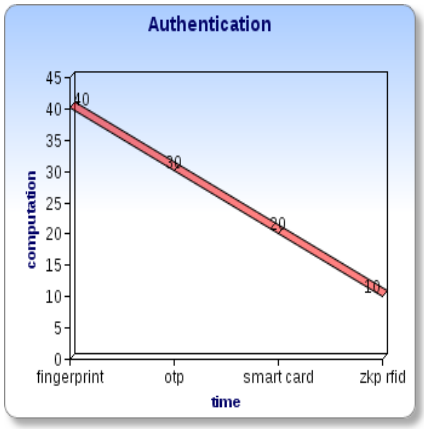


Fig: 6 performance of computation

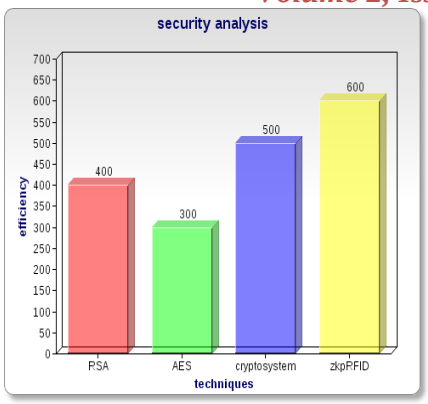


Fig: 7 Efficiency Comparison

Fig7 shows the efficiency of RFID tag with existing techniques. Efficiency of zkp in RFID shows more security than the existing authentication in social networking sites. The efficiency of ZKP RFID is compared with the existing authentication techniques such as RSA, AES and threshold cryptosystem which shows RFID as the better authentication for social networks.

VI CONCLUSION & FUTURE WORK

An authentication frame work for social networks in cloud is presented. A design for the essential authentication protocol using RFID tag allowing the use of multi factor authentication in addition to username and password is more secure with zkp privacy. It is shown that zkp privacy in RFID protocol combined with cloud computing services can offer a secure and efficient authentication. Again recall the purpose of this paper is to examine how to move beyond the traditional model of device authentication and begin to implement a more user centric approach in line with current trends in mobile network services. Only authorized users can access the tag owner's datas.The future research directions is to design Biometric authentication in the RFID tags.

REFERENCES

[1] Guomin Yang; Qiong Huang; Duncan Wong; Xiaotie Deng, "Universal authentication protocols for anonymous wireless communications," *IEEE Transactions on Wireless Communications*, vol.9, no.1, pp.168-174, Jan 2010

[2] C. Tang, "An efficient mobile authentication scheme for wireless networks" *IEEE Transactions on Wireless Communications*, vol.7, no.4, pp.1408-1416, April 2008

[3] W. Granzer, F. Praus, W. Kastner, "Security in building automation systems," *Industrial Electronics, IEEE Transactions on*, vol.57, no.11, pp.3622-3630, Nov. 2010

[4] Chun-I Fan; Pei-Hsiu Ho; Ruei-Hau Hsu, "Provably secure nested one-time secret mechanisms for fast mutual Authentication and key exchange in mobile communications," *Networking, IEEE/ACM Transactions on* , vol.18, no.3, pp.996-1009, June 2010

[5] Chu-Hsing Lin, Yi-Yi Lai, "A flexible biometrics remote user authentication scheme", Computer Standards &

Interfaces, pp. 19-23, Volume 27, Issue 1, November 2004.

[6] P. Corcoran, C. Iancu, F. Callaly, A. Cucos," Biometric access control for digital media streams in home networks", *IEEE Trans. Consumer Electron.*, vol. 53, No. 3, pp. 917-925, August 2007.

[7] P. Corcoran, A. Cucos, T. Grossman, "Biometrically auditable public key infrastructure technology for secure multimedia content," *Consumer Electronics, ICCE. 2005 Digest of Technical Papers. International Conference on*, vol., no., pp. 33- 34, 8-12 Jan. 2005

[8] P. Corcoran, A. Cucos, "Techniques for securing multimedia content in consumer electronic appliances using biometric signatures", IEEE Transactions on Consumer Electronics, Vol. 51, No. 2, pp. 545-551, May 2005.

[9] Li Xiong; Ling Liu; "Peer Trust: supporting reputation-based trust for peer-to-peer electronic communities," *IEEE Trans. on Knowledge and Data Engineering*, vol.16, no.7, pp. 843- 857, July 2004

[10] Binod Vaidya et. al "Robust one-time password authentication scheme using Smart card for home network environment." *Electronic Commerce Research and Applications*, 2011, vol. 3, No-5, pp.89-92.

[11] Slawomir Grzonkowski and Peter M. Corcoran "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking", *IEEE Transactions on Consumer Electronics, Vol. 57, No. 3, August 2011*

[12] Slawomir Grzonkowski et. al "Sharing information across community portals with FOAFRealm" *IEEE systems journal. Web Based Communities, 2009, Vol. 5, No. 3, and pp.105-108*

[13] S.R. Kruk, S. Grzonkowski, A. Gzella, T. Woroniecki and H.C. Choi. D-FOAF: distributed identity management with access rights delegation. In Procedings of Asian Semantic Web Conference, September 2006

[14] R.Chow, M. Jakobson et.al "Authentication in the clouds: a framework and its application to mobile users", in proceedings of the 2010 ACM workshop on cloud computing security workshop, CCSW'10.New York, pp.1-6.

[15] Kyle Chard et al." Social Cloud: Cloud Computing in Social Networks", *IEEE 7th International Conference on Web Services,2011*

[16] Muhammad Ali Bing etal. "Anonymous RFID authentication for cloud services *"International journal of information security science", 2011, vol.1, no.2.*

[17] A. Juels and S. Weis. Defining Strong Privacy for RFID. In International Conference on Pervasive Computing and Communications PerCom 2007.

[18] J. Ha, S. Moon, J. Zhou, and J. Ha. A new formal proof model for RFID location privacy. In European Symposium on Research in Computer Security (ESORICS) 2008, volume 5283 of Lecture Notes in Computer Science.

Sherin Jobe was born in 1988. She graduated B.E.degree in computer science & Engineering from PET Engineering College, Anna University, Chennai, TamilNadu, India in 2009.Currently pursuing M.E.degree in computer science & Engineering from Noorul Islam University, Kumaracoil, TamilNadu, India. Her research interest includes wireless communication and cloud computing.

Venifa Mini. G. B.E, M.E, doing Ph.D., Assistant Professor, Noorul Islam University, and Kumaracoil.Her research interest includes wireless network and cloud computing

J.Jeya.A.Celin.B.Sc, MCA, Ph.D., Professor her research interest includes data mining, wireless networking and cloud computing