Oct - Dec © 2015 Transactions; 2(8): 371-175

International Journal of Research and Applications

ISSN (online): 2349-0020 ISSN (print): 2394-4544 http://www.ijraonline.com/

Survey Report

A Multilevel authentication based on the RFID technique for a multiple mobile cloud user in cloud storage: A Survey

Naresh Vurukonda [1] and Dr.B.Thirumala Rao [2]

Corresponding Author:
naresh.vurukonda@gamil.com

DOI:
http://dx.doi.org/
10.17812/IJRA.2.8(63)2015

Manuscript:
Received: 2nd Dec, 2015
Accepted: 10th Dec, 2015
Published: 28th Dec, 2015

Publisher:
Global Science Publishing Group, USA
http://www.globalsciencepg.org/

ABSTRACT

Now in Modern days we can lots of mobile users. The cloud computing and mobile user is increasing day to day life. Cloud computing moves software and database applications to large central facility where management and data services that the data cannot be fully worthy of confidence. The Architecture first full gathering information encrypted, key management, and authentication and authorization solutions, dealing with relevant issues rules threat scenarios typical data for cloud computing services. Formal models describing the proposed solutions for the implementation of an access control system and ensure the confidentiality of data and metadata. We propose plans to address privacy we will continue to search for multiple keywords Ranked multi-owner model that will allow Cloud servers to perform the search safely without knowing the actual data for each of the keywords and the gates, and we are building a research methodology novel safe protocol. To organize search results and to maintain the privacy of dozens of keywords and all the similar files have a new system and the privacy of the family and plans to function added. To prevent attackers spy secret keys and pretending to be data users provide genuine work was been suggests a dynamic new generation protocol and the new secret key user authentication protocol data. Implementation of the system point of view, there is no need to check the table's intelligent generator card supports it (SCG) and providers of cloud computing services in the adoption of the proposed plan. Now we propose a RFID theme in the cloud storage system where we can implement the all the storage could be down only the with the specific RFID not only that we can also implement the RFID in a way as it can hold only the 2000bytes of data we can make it to access the cloud store as a security for the interaction of the cloud storage for an authentication and for the manipulation won't be possible without RFID those this will provide an create security for an cloud even for using for the multiple user.

Keywords: Mobile cloud computing, RFID, Wireless Network, Mobile Network, Mobile devices, Cloud computing, authentication.

[1, 2] Department of CSE, KL University, Vijayawada, A.P, India

IJRA - Year of 2015 Transactions:
Month: October - December
Volume – 2, Issue – 8, Page No's:371-375
Subject Stream: Computers

Paper Communication: Author Direct
Paper Reference Id: IJRA-2015: 2(8)371-375

DOI: 10.17812/IJRA.2.8(63)2015

International Journal of Research and Applications
Oct - Dec © 2015 Transactions 2(8): 371-375

eISSN : 2349 – 0020
pISSN : 2394 - 4544

COMPUTERS SURVEY REPORT

A Multilevel authentication based on the RFID technique for a multiple mobile cloud user in cloud storage: A Survey

Naresh Vurukonda [1], Dr.B.Thirumala Rao [2]

[1, 2] Department of CSE, KLUniversity,Vijayawada, A.P, INDIA
[1] ,naresh.vurukonda@gamil.com [2] thirumail@yahoo.com

ABSTRACT

Now in Modern days we can lots of mobile users. The cloud computing and mobile user is increasing day to day life. Cloud computing moves software and database applications to large central facility where management and data services that the data cannot be fully worthy of confidence. The Architecture first full gathering information encrypted, key management, and authentication and authorization solutions, dealing with relevant issues rules threat scenarios typical data for cloud computing services. Formal models describing the proposed solutions for the implementation of an access control system and ensure the confidentiality of data and metadata. We propose plans to address privacy we will continue to search for multiple keywords Ranked multi-owner model that will allow Cloud servers to perform the search safely without knowing the actual data for each of the keywords and the gates, and we are building a research methodology novel safe protocol. To organize search results and to maintain the privacy of dozens of keywords and all the similar files have a new system and the privacy of the family and plans to function added. To prevent attackers spy secret keys and pretending to be data users provide genuine work was been suggests a dynamic new generation protocol and the new secret key user authentication protocol data. Implementation of the system point of view, there is no need to check the table's intelligent generator card supports it (SCG) and providers of cloud computing services in the adoption of the proposed plan. Now we propose a RFID theme in the cloud storage system where we can implement the all the storage could be down only the with the specific RFID not only that we can also implement the RFID in a way as it can hold only the 2000bytes of data we can make it to access the cloud store as a security for the interaction of the cloud storage for an authentication and for the manipulation won't be possible without RFID those this will provide an create security for an cloud even for using for the multiple user.

Keywords: Mobile cloud computing, RFID, Wireless Network, Mobile Network, Mobile devices, Cloud computing, authentication.

1. INTRIDUCTION

RFID systems consist of small radio chips in tags placed on items, as well as readers that can recognize the emitted signals. Most commercial RFID chips, such as those used in place of bar codes on products in stores, are passive emitters and thus have no onboard power source. They send a signal over a range of several feet when a nearby reader activates them. Active emitter chips, like those used in automatic highway toll-paying devices that let drivers pass through collection booths without stopping, have their own batteries and thus can send signals up to about 300 feet to readers. RFID transceivers, such as the one that Figure 1 shows, are tiny, resource- constrained computers. In passive systems, they detect a signal arriving from a reader, power up the tag, send a reply, and store a small amount of data. The amount of storage depends on the usage, varying from a few bits for applications such as a small store's inventory-control system to multiple kilobits for applications such as a large business supply-chain system. The readers perform various functions, like simply displaying data such as a product's price, acting on data such as admitting a person to a building, or communicating with a back-end application such as a toll system's database. The data in some RFID tags, such as those used to store product prices, is read-only. Other tags are read write, so information can be stored as the need arises. For example, this type of system could write location and other information about a product to a tag as it moves through a supply chain, explained Jack Brandon, manager of business development for Socket Communications, a vendor of data-collection and network-connectivity products for mobile devices. Because RFID is simple, it is generally inexpensive, which is practical for use in high-volume settings such as stores and warehouses. Even though RFID chips have little memory, they can send malicious data to unsecured back-end databases and other systems that are susceptible to common attacks such as viruses, buffer overflows, and denial-of-service (DoS) ssaults, said Vrije Universiteit's Rieback. "Of even greater concern can be the lack of definitive binding between the tags and the objects they purportedly correspond to," added SRI International's Neumann. For example, he said, terrorists or smugglers could switch tags or disable one tag and add another to evade future RFID-based airport luggage-scanning systems. Edith Cowan University's School of Computer and Information Science Security Research Group says it showed how hackers could launch DoS attacks against some types of RFID systems, including those in which tags communicate via frequency- hopping spread-spectrum modulation. FHSS entails the repeated switching of frequencies during transmission, which reduces interference and makes intercepting signals more difficult. The Edith Cowan researchers used RF jamming, which sends signals across the entire spectrum range in which an FHSS-based RFID system functions, explained university lecturer Andrew Woodward. This technique continuously sent signals to an RFID tag, which left it unable to respond to or communicate with legitimate traffic. The security strength of the proposed scheme is based on bilinear pairing cryptosystem and dynamic nonce generation. In addition, the scheme supports mutual authentication, key exchange, user anonymity, and user intractability. From system implementation point of view, verification tables are not required for the trusted smart card generator (SCG) service and cloud computing service providers when adopting the proposed scheme. In consequence, this scheme reduces the usage of memory spaces on these corresponding service providers. In one mobile user authentication session, only the targeted cloud service provider needs to interact with the service requestor (user). The trusted SCG serves as the secure key distributor for distributed cloud service providers and mobile clients. In the proposed scheme, the trusted SCG service is not involved in individual user authentication process. With this design, our scheme reduces authentication processing time required by communication and computation between cloud service providers and traditional trusted third party service. Formal security proof and performance analyses are conducted to show that the scheme is both secure and efficient.

2. RELATED WORK

Cloud computing has generated significant interest in both academia and industry, but it's still an evolving paradigm. Essentially, it aims to consolidate the economic utility model with the evolutionary development of many existing approaches and computing technologies, including distributed services, applications, and information infrastructures consisting of pools of computers, networks, and storage resources. Confusion exists in IT communities about how a cloud differs from existing models and how these differences affect its adoption. Some see a cloud as a novel technical revolution, while others consider it a natural evolution of technology, economy, and culture.1 Nevertheless, cloud computing is an important

1

paradigm, with the potential to significantly reduce costs through optimization and increased operating and economic efficiencies.1, 2 Furthermore, cloud computing could significantly enhance collaboration, agility, and scale, thus enabling a truly global computing model over the Internet infrastructure. However, without appropriate security and privacy solutions designed for clouds, this potentially revolutionizing computing paradigm could become a huge failure. Several surveys of potential cloud adopters indicate that security and privacy is the primary concern hindering its adoption.3 this article illustrates the unique issues of cloud computing that exacerbate security and privacy challenges in clouds.4 we also discuss various approaches to address these challenges and explore the future work needed to provide a trustworthy cloud computing environment. The technology behind RFID has been in use since World War II, when the British used it to identify whether planes belonged to “friend or foe.” Work on the technology continued, and in 2004, vendors began pilot projects using RFID tags on products and supplies to store pricing- and inventory-related information, said Bert Moore, AIM’s director of communications and media relations. Large institutions, such as the US Department of Defense, have since implemented RFID, which is now spreading to other organizations and industries. Despite increasing usage of mobile computing, exploiting its full potential is difficult due to its inherent problems such as resource scarcity, frequent disconnections, and mobility. Mobile cloud computing can address these problems by executing mobile applications on resource providers external to the mobile device. In this paper, we provide an extensive survey of mobile cloud computing research, while highlighting the specific concerns in mobile cloud computing. We present a taxonomy based on the key issues in this area, and discuss the different approaches taken to tackle these issues. We conclude the paper with a critical analysis of challenges that have not yet been fully met, and highlight directions for future work. There are tremendous business prospects for the cloud computing application on mobile internet. But combining cloud computing technology into mobile internet gives birth to a serial of security problems. One of the challenges is to construct the cloud computing secure architecture on mobile internet. After analyzing the available cloud computing security risks and secure architectures, and taking into account the characteristics of mobile internet, this paper designs a general secure cloud computing architecture on mobile internet with the advantages such as multi-hierarchy, multi-level, elasticity, cross-platform and unified user interface. The future Internet is a term commonly related to research topics on new architecture for Internet. In fact, the Internet of tomorrow will rely on virtualization and cloud networking, which open the door for new security threats and attacks and address many problems related to identification, authentication, secure data transfer, and privacy in virtual networks and clouds. The purpose of our work is to define architecture for strong authentication and identity management in virtual networks using EAP-TLS smart cards technology. The architecture is based on a Grid of EAP-TLS smart cards, as an authentication server, able to manage users’ access to their virtual networks by authenticating either the user or the virtual network.

3. SYSTEM PREMELIRIES

A. MOBILE USER:

The user can access with the cloud storage with the help of the data provided by the user to cloud the cloud will generate the an key which will be included in the preparation and creation of the RFID, here the user can store, manipulate and manage of all the operation could be only possible with the help of the RFID code which was purely developed by the monitor.

B. MONITOR

Here the monitor will access all the information of i.e log information and the details of all the users and he will be the responsible for the maintain ace of the generation and the creation of the cloud id and the RFID for the particular user.

1

C. RFID

The RFID will be generated cloud be generated based on the cloud storage and the details which provided by the client the code which was generated by the RFID will be very unique with the combination of the letter and number, where it couldn't able to decrypted easily. At the time access the particular data from the cloud storage are the place the particular data in the cloud storage the only the RFID would be helpful to access the cloud storage.

4. PROPOSED SYSTEM DESIGN

In this system we are implementing the technique, which authenticates cloud storage data at multiple levels so, we generates passwords at multiple levels and then concatenates them into one single password. Hence Authentication activities take place in multiple levels like organization, team and user levels. User has to go through different levels of the authentication, First authentication will ask for the user id and password which defines that user is authenticated or not, second level will assign the number of resources for team member and last one defines the access rights for the resources. It reads the authentication password and checks to authenticate the organization for cloud access. Providing different password at different levels of management, developer and user according to their accessing rights. Also providing data sharing, symmetric key (AES) & asymmetric key (RSA) and its combination for data encryption technique for the purpose of improving data security.

5. IMPLEMENTATION

This technique authenticates the cloud access in multiple levels. It generates the password and joins and produces password at multiple levels. Based on the leaf level join password, one can access the cloud services provided that the password authentication is successful in all the existing levels. This technique has two separate entities: i) Cloud service provider, who provides the cloud services and ii) Authenticated client organizations that access the cloud services (Before using cloud services, company authentication confirms with service agreement and other formal procedure from cloud vendors). This architecture helps in checking the authentication against the services and privileges. It also helps to ensure which customer has what kind of privileges to use cloud services. This is evaluated by multiple levels authentications. First level of authentication is organization level password authentication/generation. It is for okay the cloud access authentication from cloud vendor. If unauthenticated organization or intruder tries to access the cloud services, they are going to abolish in this level itself. Second level of authentication is a team level password authentication/ generation. It is to authenticate the team for particular cloud service. Like this, authentication system can have third, fourth, fifth etc level. Finally, the last level will be the user level password authentication/generation, which ensures that customer/end user has particular privileges and permission.

6. CONCLUSION

We conclude that we propose a RFID theme in the cloud storage system where we can implement the all the storage could be down only the with the specific RFID not only that we can also implement the RFID in a way as it can hold only the 2000bytes of data we can make it to access the cloud store as a security for the interaction of the cloud storage for an authentication and for the manipulation won't be possible without RFID those this will provide an create security for an cloud even for using for the multiple user. 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 data.

REFERENCES

[1] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: A survey," Future Gen. Comput. Sys. vol. 29, no. 1, pp. 84–106, Jan. 2013.

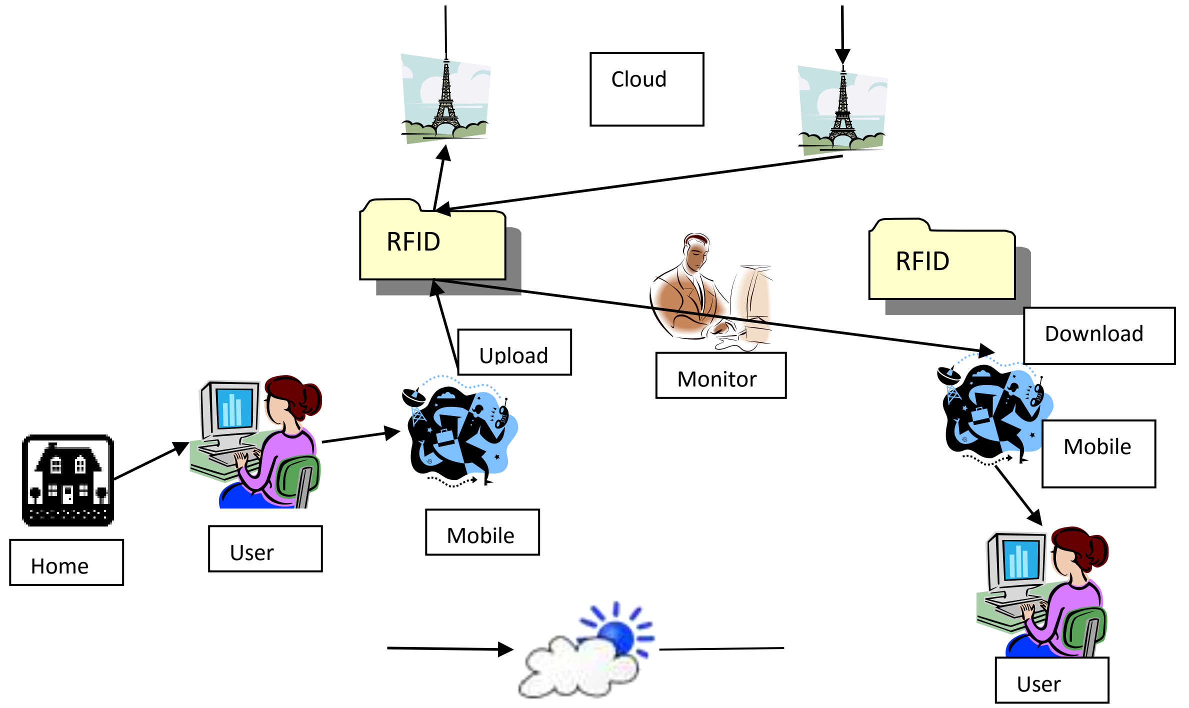

Fig 1: Working Model OF RFID IN Cloud Storage

[2] G. Le, K. Xu, M. Song, and J. Song, "A survey on research on mobile cloud computing," in Proc. 10th IEEE/ACIS/Int. Conf. Comput. Inf. Sci., 2011, pp. 387–392.

[3] X. F. Qiu, J.W. Liu, and P. C. Zhao, "Secure cloud computing architecture on mobile Internet," in Proc. 2nd Int. Conf. AIMSEC, 2011, pp. 619–622.

[4] W. G. Song and X. L. Su, "Review of mobile cloud computing," in Proc. IEEE 3rd ICCSN, 2011, pp. 1–4.

[5] ABI Research Report, Mobile Cloud Applications. [Online]. Available: http://www.abiresearch.com/research/1003385-Mobile+Cloud+ Computing.

[6] P. Urien, E. Marie, and C. Kiennert, "An innovative solution for cloud computing authentication: Grids of EAP-TLS smart cards," in Proc. 5th Int. Conf. Digit.Tel. 2010, pp. 22–27.

[7] H. Ahn, H. Chang, C. Jang, and E. Choi, "User authentication platform using provisioning in cloud computing environment," in Proc. ACN CCIS, 2011, vol. 199, pp. 132–138.

[8] H. Chang and E. Choi, "User authentication in cloud computing," in Proc. UCMA CCIS, 2011, vol. 151, pp. 338–342.

[9] J. L. Tsai, N. W. Lo, and T. C. Wu, "Secure delegation-based authentication protocol for wireless roaming service," IEEE Commun. Lett. vol. 16, no. 7, pp. 1100–1102, Jul. 2012.

[10] W. Itani, A. Kayssi, and A. Chehab, "Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures," in Proc. IEEE Int. Conf. Dependable Auton. Secure Comput., 2009, pp. 711–716.

[11] S. Pearson, "Taking account of privacy when designing cloud computing services," in Proc. CLOUD ICSEWorkshop Softw. Eng. Challenges Cloud Compute. 2009, pp. 44–52.

[12] Miss.Sneha Khomeshwar Khodake "Multi-level Authentication Technique for Accessing Organization in Cloud Data."International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 12, December 2014. ISSN 2348 – 4853 195 | © 2014, IJAFRC All Rights Reserved www.ijafrc.org.

[13] Sherin Jobe, Venifa Mini.G and Jeya A.Celin J." Efficient RFID Authentication in Cloud Computing" ISSN: 2278 – 7798 International Journal of Science, Engineering and Technology Research (IJSETR) Volume 2, Issue 4, April 2013.