IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-2, Issue-12 E-ISSN: 2347-2693

Achieving Security in Ad hoc Networks Using Identity and Trust with Key Management

Pranav Nair[1*], Archana Jadhav[2] , Swapnaja Gunjal[3] and Ruchita Gadsing[4]

[*1,2,3,4]*Department of Information Technology, University of Pune, India,*

pranavnair.925@gmail.com , kadamarchana@rediffmail.com , gunjal.swapnaja123@gmail.com , ruchita.gadsing18@gmail.com

www.ijcaonline.org

Received: Nov /26/2014 Revised: Dec/04/2014 Accepted: Dec/22/2014 Published: Dec/31/ 2014

Abstract— A Network user has to provide susceptible personal information (e.g. name, residence address, credit/debit card number, contact number, driver's license number and date of birth, etc.) when they are requested by some Web page. This exclusive Personal Identity Information may be used to exclusively identify, contact and/or locate a particular user. This information may be exploited and abused if not properly protected. An Identity Management (IDM) system is therefore proposed to overcome this problem and helps to decide the access to this information in a secure manner. The concept of key management has been implemented to achieve the goal of trusted communication. The group public key management scheme, trust of a node and physical identity helps in secure data transfer over wireless channels through the concept of composite identity and trust based model(CIDT). To validate a node in the network Trust Factor of a node along with its key pair and identity is used. Proposed method works well for self certification scheme of a node in the network.

Keywords— *Personal Identity Information(PII), Identity Management(IDM), Service Provider(SP), Trusted Third Party(TTP)*

I. Introduction

Many information of a particular individual may consists of personal documents likes photos and videos; files and documents; bank details, appointments etc. which can be stored on the web instead of storing them locally on a computer.

The information about another entity is maintained by a third party i.e. A Web service provider (SP). Assuming that a Trusted Third Party (TTP) will perform its task as it is expected posses a great risk because it may not be true all the time. Privacy or confidentiality questions may arise whenever some entity stores or processes information in the cloud.

Much information is stored in the cloud and they are revealed only when required, but it depends on the entities to give only the desired information about itself to the cloud or the Service Provider (SP) and it should control who can access that information. This concept can be termed as privacy in network computing.

Communication in Mobile network is done over a shared wireless channel. Responsibility of maintaining the veracity and privacy of data and nodes in the network are held responsible. A lot of approaches using key management has been implemented to attain the goal of trusted communication. The group public key management scheme, physical identity and trust of a node helps in secure data transfer over wireless channels and proposes a composite identity and trust based model (CIDT) which depends on it. Trust Factor of a node along with its key pair and identity is used to authenticate a node in the network. A valid certificate is generated for authentic node to carry out the communication in the network. Self certification scheme of a node in the network works well by this proposed method.

The use of Internet based services in network computing is used to support business processes and rental of IT-services on a value-like basis .It offers an awareness of resources but it can also pose a high risk for data privacy. A single violation can cause significant loss. Entities may have multiple accounts in Identity management computing and each of these accounts may be associated with single or multiple service providers.

Corresponding Author: *Pranav Nair*

II. LITERATURE SURVEY

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). Remote services are entrusted by cloud computing with a user's data, software and computation.

The cloud computing holds the potential to eliminate the requirements for setting up of high cost computing infrastructure for the IT-based services that the industry uses. It provides a flexible IT architecture, accessible through internet for lightweight portable devices. It allows many-fold increase in the capabilities or capacities of the existing and new software is allowed. In cloud computing environment, entire data reside over a set of resources, which are connected in network, which enables the data to be accessed through virtual machines. These data centers may lie in any corner of the world beyond the reach of users and users cannot control it still there are multifarious securities, privacy challenges which are to be handled and taken care of. It may possible that breakdown of a server occurs that has been witnessed, rather quite often in the recent times cannot be ignored. There are various issues with respect to security and privacy in a cloud computing scenario need to be dealt with.

Cloud computing allows the use of Internet-based services to support business processes and rental of IT-services on a utility-like basis. It not only offers the concentration of resources but also poses risks for data privacy. A single breach can cause significant loss. A danger of multiple, collaborative threats are represented by heterogeneity of "users". One person may have multiple accounts in cloud computing, related with a single or multiple service providers (SPs). Sharing sensitive identity information (Personally Identifiable information (PII)) along with associated attributes of the same person across services can lead to mapping of the identities to the person, which may lead to the loss of privacy. Identity management (IDM) is one of the core components in cloud privacy, security and can help to make some of the problems less severe. There are solutions used by TTP which lets SP to identify people who are available. The usages of solutions on entrusted hosts are not recommended by solution providers. We introduce an approach for IDM that has the ability to use identity data on entrusted hosts which is independent on TTP's. The approach is dependent on the use of predicates over encrypted data and multi-party computing for negotiating the use of cloud service. It uses active bundle—which the middleware agent that has PII data, privacy policies, a virtual machine that will enforce the policies, and has a set of protection technique to protect itself.

On behalf of a user, an active bundle will communicate, for authentication of cloud services using user's privacy policies.

III. RELATED WORK

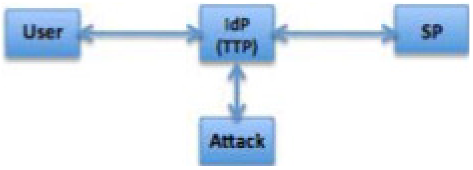
We looked towards the most hackneyed answers from IDM:

1) PRIME: Retreat Privacy and Identity Management for Europe (PRIME) gives privacy sustaining authentication using a Trusted Third Person (TPP), named IdP.

2) Windows CardSpace: Windows CardSpace negotiates total digital identity as a security token, which consists of a rigid declarations (such as username, address, mobile number, SSN, etc). The reminders show to Service Provider(SP) that the claims belong to the user presenting them.

3) Open ID: Open ID is a decentralized authentication protocol that helps cloud users in managing their many digital identities and it provides a greater control to manage their sharing of private identity information.

A user has to think individual username moreover password-an Open ID-and can log on websites beside this OpenID.



Different answers employ different approaches of sending user's PII for placement beside the SP's. The common accesses are:

1) Benefit of a Trusted Third Party (TTP). Most of the keys that we studied use TTP for approving or verifying PII. The major issues accompanying such advance in cloud computing are given below:

a) TTP could be a cloud service, hence SP could also be TTP consequently, TTP might not be an independent trusted entity anymore.

b) Using a single TTP is a centralized avenue beside its inherent danger that compromising TTP decisions in compromising all PIIs of its users as well.

2) Prohibiting Entrusted Companies, A customer relevance holding PII want be executed on a trusted network to suppress malicious hosts from accessing PII.

SELECTED SEARCH PROBLEM

The research dilemmas that we approach in this paper are:

1) Authenticating without disclosing PII: Whenever the user forwards PII to authenticate for a service, the user might encrypt it. Nevertheless, PII is decrypted prior an SP uses it. The moment PII is decrypted, it can be attacked easily.

2) Using benefits on entrusted hosts: There are IDM solutions available which requires user to execute IDM from trusted host. Use of IDM on entrusted hosts, such as
Public hosts are not recommended.

Therefore, in cloud computing data may reside anywhere in cloud or in host, this issue needs to be addressed. E.g. User herself might be on a cloud Virtual Machine.

IV. PROPOSED MODEL

Some of the main problems in cloud computing involves security and privacy in cloud and Identity Management (IDM) is considered as one of the most important components that can solve these problems. Cloud computing has helped in providing and delivery of services over the network and also helped in working of computation and data from terminal devices and local servers to core data centre due to flexibility, economics of saving and scalability. These services are mostly supported by datacenters located at various distant location located at various sites. However, the security still remains a major concern in these infrastructures even though the benefits of cloud computing is clear. Access to an organizations data and resources can be achieved only by an authorized user having a privileged user access. Therefore, a security concern in cloud computing may be identity and access management. Central Identity and Access management (IAM) , Trusted Third party (TTP) and federation solutions etc. are the various models that have been proposed to address identity management in cloud computing. Federation of cloud providers and paying less or no attention to access management are the solutions that are mainly focused on. In this system, we propose a new architecture to manage identity and control access to resources in a cloud infrastructure. First, we discuss system requirements and then we propose architecture to address these requirements. Middleware and central IAM are the two major components that are used to manage user and infrastructure related data in the proposed model architecture. Middleware sits in front of a resource provider and handles time-consuming decision making such as authentication and authorization, while the repository handles data manipulation without disclosing the user identity.

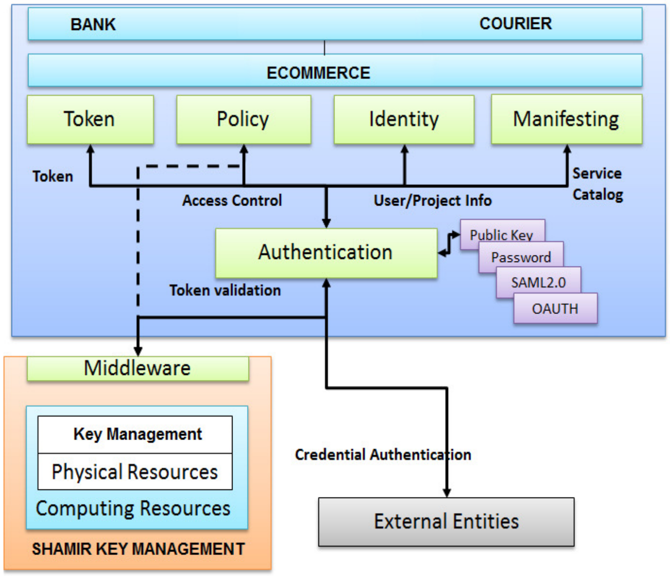


Fig: Proposed System Architecture

Here in the system architecture we describe the proposed IDM approach which uses the active bundle scheme, multi-party computing and computing predicates over encrypted data.

The Key features of IDM approach are :

1) We can authenticate the data without disclosing unencrypted data by using predicate over encrypted data.

2) By using an active bundle scheme we can use identity data on entrusted hosts. A complete self destruction called 'apotosis' and a partial self-destruction called 'evaporation' when the check fails are the self-integrity check mechanism of an active bundle.

3) By using multi-party computing where secrets are split into shares distributed to different hosts will help in achieving the independence of TTP's.

4) To give answers to predicate about PII we use multiparty computing and predicates with encrypted data.

Here, in the proposed model we use the technique of Shamir's Algorithm. The threshold of secret sharing is given by Shamir.

Shamir Algorithm is a form of secret sharing technique. Here, the secrets are divided into number of parts and each participant is given its own unique part. To reconstruct this secret we need some or all of the parts that were given to each participant.

Sometimes it may be difficult to get the divided parts from all the participants at the same time and therefore reconstructing secret would be impractical. Hence, sometimes the use of threshold scheme is done where any k of the parts are sufficient to reconstruct the original secret.

Mathematical definition:

The secret S is divided into n pieces of data $D1,\ldots,Dn$ in a way that:

1) S is easily computable only if we have knowledge of any k or more Di pieces.

2) S is completely undetermined if we have knowledge of any $k\text{-}1$ or fewer Di pieces.

This threshold scheme is called (k,n).

All participants are required to reconstruct the secret if $k=n$.

V. CONCLUSION

In this project, we have introduced a novel architecture for a cloud-based IDM. Our architecture uses a central IDM and middleware to carry out Security and Ecommerce duties. The main features in this architecture are scalability, security in access control by implementing Key Management Protocol, and extensibility to future technologies. The Key Management Shamir's Protocol introduces great flexibility in selecting authentication method by designing a common Pluggable Authentication module. It also introduces an open platform for authorization and delegation that is an essential requirement for an application-centric infrastructure. Our experiment shows that the IDM improves the throughput of as the system stands more secure. In the future, we plan to study federation to enable bursting to other cloud providers.

We are also interested in including new authentication technologies such as QR-Code and mobile device into IDM.

REFERENCES

[1] Pallavi Khatri, "Using Identity and Trust with Key Management for achieving security in Ad hoc Networks" INDIA, _c 2014 IEEE

[2] Shibin Chen , Lingfang Zeng , Qingsong Wei and Dan Feng, SeDas:- A Self-Destructing Data System Based on Active Storage Framework", China,2013 IEEE

[3] R. Geambasu, T. Kohno, A. Levy, and H. M. Levy, “Vanish: Increasing data privacy with self destructing data,” in *Proc. USENIX Security Symp.*, Montreal, Canada, Aug. 2009, pp. 299–315

[4] A. Shamir, “How to share a secret,” *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[5] S. Wolchok, O. S. Hofmann W. Felten, J. A. Halderman, C. J. Rossbach, B. Waters, and E. Witchel, “Defeating vanish with low-cost sybill attacks against large DHEs,” in *Proc. Network and Distributed System Security Symp.*, 2010.

[6] L. Zeng, Z. Shi, S. Xu, and D. Feng, “Safevanish: An improved data self-destruction for protecting data privacy,” in *Proc. Second Int. Conf. Cloud Computing Technology and Science (CloudCom)*, Indianapolis, IN, USA, Dec. 2010, pp. 521–528.

[7] J. R. Douceur, “The sybil attack,” in *Proc. IPTPS ’01: Revised Papers From the First Int. Workshop on Peer-to-Peer Systems*, 2002.

[8]. C.E. Perklins, “Ad Hoc Networking”, 1st edition. Addison –Wesley Professional, 2001.

[9]. I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," Computer Networks, Volume 47, 2005, pp. 445-487.

[10]. H. Dahshan, and J. Irvine, “A trust based threshold cryptography key management for mobile ad hoc networks,” *IEEE 70th Vehicular Technology Conf.*, Anchorage, AK, USA, pp. 1-5, Sept. 2009,.

[11]. S. Capkun, L. Buttya, and J.-P. Hubaux, “Selforganized public-key management for mobile ad hoc networks,” *IEEE Transactions on Mobile Computing*, vol. 2, no. 1, pp. 52-64, Jan. – Mar., 2003.

[12]. B.J. Chang and S.L. Kuo, “Markov chain trust model for trust-value analysis and key management in distributed multicast MANETs,” *IEEE Transactions on Vehicular Technology*, vol. 58, no. 5, pp. 1846-1863, May 2009.

[13]. A. Shamir, “Identity-Based Cryptosystems and Signature Schemes,” *CRYPTO‘84*, 1984, pp. 47–53.

[14]. Y. G. Desmedt, “Threshold cryptography,” European Transactions on Telecommunications, vol. 5, no. 4, pp. 449-458, July/Aug. 1994.

[15]. J. Huang and D. Nicol, “application to PKI and IDM with calculus of trust,” *ACM 8th Symposium on Identity and Trust on the Internet*, Gaithersburg, MD, USA, April 2009.

[16]. B. Poettering, 2006, SSSS: Shamir’s Secret Sharing Scheme [Online]. Available: http://point-at-infinity.org/ssss/

[17]. Khatri, P., Tapaswi, S. & Verma, U.P. (2012). Trust evaluation in wireless ad hoc networks using fuzzy system. In V. Potdar & D. Mukhopadhyay (eds.), pp.779-783, CUBE 2012.