International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Consolidated Identity Management System for Secure Mobile Cloud Computing

P.R.Menaka
Computer Science Department
M.A.M College of Engineering from Trichy

Abstract- Privacy and security in cloud computing is an important concern for both the public and private sector. Cloud computing allows the use of internet-based services to support business process and rental of IT services on a utility-like basis. While cloud computing offers a massive concentration of resources, it poses risks for privacy preservation. The expected loss from a single breach can be significant and the heterogeneity of "users" represents an opportunity of multiple, collaborative threats. Problems associated with trusted 3rd party managed Cloud Computing stem from loss of control, lack of trust (mechanisms) and multi-tenancy. Identity management (IDM) is one of the core components in cloud privacy and security and can help alleviate some of the problems associated with cloud computing. Cloud computing requires a user-centric access control where every user's request for any provider is accompanied with the user identity and entitlement information. The system creates digital identities for its users, and protects the users' Personally Identifiable Information (PII). User identity has identifiers or attributes that constitute PII, which identifies and defines the user. The identity is portable although tied to a domain. This user-centric approach gives the users the ultimate control of their digital identities. We propose and validate a new IDM architecture dubbed Consolidated IDM (CIDM) that countermeasures these attacks. We discuss and propose approaches for privacy preservation in the cloud that does not use a trusted third party. The components of the proposed approach are: (i) use of active bundle—which is a middleware agent that includes data, privacy policies and a virtual machine that enforces the policies and use a set of protection mechanisms (i.e., integrity check, apoptosis, evaporation, decoy) to protect itself, as a container for PII; (ii) use of active bundle to mediates interactions between the user and cloud services using user's privacy policies; and (ii) use of predicate over encrypted data computing when negotiating a use of a cloud service.
Keywords: IDM system, Multi tenancy, Data encryption, Predicted data

I. INTRODUCTION

Cloud computing is Internet-based computing, whereby shared resources, software and information are provided to computers and other devices on-demand, like the electricity grid. The cloud computing is a culmination of numerous attempts at large scale computing with seamless access to virtually limitless resources.On demand computing, utility computing, ubiquitous computing, autonomic computing, platform computing, edge computing, elastic computing, grid computing, … The term "cloud" appears to have its origins in network diagrams that represented the internet, or various parts of it, as schematic clouds. "Cloud computing" was coined for what happens when applications and services are moved into the internet "cloud." It is a pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end-customer applications and billed by consumption. A paradigm in which information is permanently stored in servers on the Internet and cached temporarily on clients that include desktops, entertainment centers, table computers, notebooks, wall computers, handhelds etc. Cloud computing may trace back to a time when computer systems remotely time-shared computing resources and applications. More currently though, cloud computing refers to the many different types of services and applications being delivered in the internet cloud, and the fact that, in many cases, the devices used to access these services and applications do not require any special applications.

II. RELATED WORK

L.A. Martucci, A. Zuccato [3] investigates man-in-the-middle attacks and Denial of Service (DoS) attacks toward 802.16e-basedMobile WiMAX network. We find the initial network procedure is not effectively secured that makes Man-in-the-middle and Dos attacks possible. In addition, we find the resource saving and handover procedure is not secured ENOUGH to resist DoS attacks. Focusing on these two kinds of attacks, we propose Secure Initial Network Entry Protocol (SINEP) based on Diffie-

Hellman (DH) key exchange protocol to enhance the security level during network initial. We modify DH key exchange protocol to fit it into mobile WiMAX network as well as to eliminate existing weakness in original DH key exchange protocol. A. Khreishah, S. Bouktif [2] analyzes the potential security challenges and riskscloudsmay face. In this paper, a number of security challenges, concerns and issues are discussed, including three major aspects of security, namely confidentiality, integrity and availability. Broad band wireless access solutions by taking advantage of the inherent mobility of wireless media.I. Berni, B. Markelj [4] implement new protective measures that are constantly under development, but changes and adaptations will always be needed. Corporations should adopt efficient safety policies and continuously educate employees about potential hazards in cyberspace.M. Leandro, T. Nascimento [1] implemented the negative impact on user's security in the case of illegal mobile device capture/compromise is twofold: (1) Local private data stored on the device is exposed (most of the users usually save passwords and other sensitive data in their mobiles, refer to Section 4 for more details), and (2) any data or service (e.g., over the cloud or private corporate) that can be accessed by the credentials stored on the stolen device becomes vulnerable.

A. IDMs vulnerabilities

Three vulnerabilities in the architecture of the current IDMs. The first vulnerability lies in the possibility of compromising IDM servers. Through IDM server compromise, we assume that the attacker can capture any token from within the IDM servers. IDM servers are supposed to be hard to compromise because they are likely to be protected by physical security measures, insider activity monitoring, tight access control measures, and regular logs and auditing practices. The second vulnerability lies in the ease of mobile device capture/compromise through theft, lost, or malicious mobile code injection. Mobile malicious malware becomes a very severe fast growing threat. The negative impact on user's security in the case of illegal mobile device capture/compromise is twofold: (1) Local private data stored on the device is exposed (most of the users usually save passwords and other sensitive data in their mobiles, refer to Section 4 for more details), and (2) any data or service (e.g., over the cloud or private corporates) that can be accessed by the credentials stored on the stolen device becomes vulnerable. The third vulnerability lies in the possibility of intercepting and cryptanalyzing IDM messages while being exchanged during the process of trust establishment between the user and the CSP. If an attacker intercepts the network traffic exchanged among the IDM provider, the CSP and the user, he can gain unauthorized access to user's credentials. These credentials can further be used to gain unauthorized access to cloud services and data.

B) Consolidated Identity Management System (CIDM)

1) *IDM server compromise:* We propose that user access to the CSP should only be allowed upon the successful reception of two different but related pieces of information. The first piece of information comes to the CSP directly from the client and is called the session commit value (M). The second piece of information is passed to the CSP from the client through the IDM and is called the encrypted session commit value (C). The idea is to keep the first piece of information (M) out of the access of possible IDM insiders.

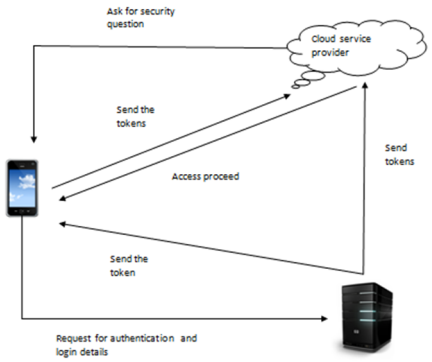
2) *Mobile client compromise:* The user generates a random symmetric key (K). The user then generates a session commit value (M) that includes her ID, the ID of the service provider, the ID of the IDM and a random nonce. The random nonce is included to prevent replay attacks. The user encrypts M using the key K to compute C (C = E (K, M)).The user login to the IDM provider using her login account with the IDM provider. The user sends C confidentially to the IDM provider (for example by encrypting it using his login password) and requests an access token to the CSP. The IDM provider generates a token, attaches C to the token, and sends the compound message to the CSP.The IDM provider sends the token to the user. The CSP presents a security question to the user .The user encrypts M and K using the public key of the service provider (Ku) to compute R (R = E(M||K, Ku). The user then sends R, the answer to the security question, and the token to the CSP. The CSP uses his private key (Kr) to decrypt R and get M and K. Then, the CSP computes Ct = E(M, K). Finally, the CSP verifies the token received from the IDM, verifies that Ct = C, and verifies the answer to the security question. If all the previous checks pass, the user is granted the requested data or service.

3) *Network traffic interception***:** The generic IDM architecture all the links among the parties carry the token. The link between the client and the CSP. Caries the proof of ownership of the session commit value (M) and the token. The link between the client and the CIDM provider carries the encrypted session commit value (C) and the token. The link between the CIDM provider

Volume 3 Issue III, March 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

and the CSP carries the token and C.

4) *Performance analysis:* Here develop a new IDM architecture dubbed consolidated IDM (CIDM) that countermeasures these vulnerabilities. Our countermeasures include: Separating the authorization credentials and distributing them among all the IDM parties (the user, the IDM provider, and the CSP) to prevent illegal access in case of IDM compromise or traffic interception, Adding a second layer of authentication using human-based challenge-response to guard against mobile device compromise, and consolidation the security of the communication link between the CIDM and the CSP to decrease the probability of successful compromise of that link. Finally, we conducted experiments to evaluate and compare the possibility of successful illegal accesses to the CSP on behalf of legitimate users for both IDM and CIDM. Our experiments show that the security provided by CIDM outperforms that provided by the current IDM systems without incurring significant computation or communication overhead.User logs in with CIDM and sends C along with login information (encrypted commit value size is 16 bytes + 20 password and username + 4 to reach minimum packet size). CIDM sends token and C to CSP (50 + 16 bytes). CSP asks user for M and K and the security question (40 bytes).User sends M, K, and ASQ encrypted with public key of CSP (64 bytes with 512 bytes public key).



II. CONCLUSION

Our analysis and experiments show that the current IDMs do not provide adequate security guarantees for mobile cloud computing. In this paper, we initially discuss the security vulnerabilities and the privacy issues of the current traditional IDMs, especially in mobile client environments. Then, we propose and evaluate a new IDM architecture dubbed Consolidated IDM (CIDM) that addresses the coupled challenges of mobility and identity management in mobile cloud computing. In this work, we assume an attack model in which the attacker's goal is to gain unauthorized access on behalf of a legitimate user. Therefore, we do not consider DoS or DDoS attacks in which the attacker tries to prevent a legitimate user from being able to prove its identity.The user generates a random symmetric key (K). The user then generates a session commit value (M) that includes her ID, the ID of the service provider, the ID of the IDM and a random nonce. The random nonce is included to prevent replay attacks. The user encrypts M using the key K to compute C (C = E(K, M)). The user login to the IDM provider using her login account with the IDM provider. The user sends C confidentially to the IDM provider (for example by encrypting it using his login password) and requests an access token to the CSP.The IDM provider generates a token, attaches C to the token, and sends the compound message to the CSP The IDM provider sends the token to the user.The user encrypts M and K using the public key of the service provider (Ku) to compute R (R = E(M||K, Ku). The user then sends R and the token to the CSP.The CSP uses his private key (Kr) to decrypt R and get M and K. Then, the CSP computes Ct = E(M, K). Finally, the CSP verifies the token received from the IDM and verifies that Ct = C. If the previous two checks pass, the CSP grants the requested access to the user.

REFERENCES

[1] R.H. Weber, A. Darbellay, Legal issues in mobile banking, J. Bank. Regul. 11 (2) (2010) 129–145.
[2] L.A. Martucci, A. Zuccato, B. Smeets, S.M. Habib, T. Johansson, N. Shahmehri, Privacy, security and trust in cloud computing: the perspective of the telecommunication industry, in: The 9th International Conference on Ubiquitous Intelligence Computing and the 9th International Conference on Autonomic Trusted Computing (UIC/ATC), 2012, pp. 627–632.
[3] B. Markelj, I. Bernik, To use or not to use mobile devices, J. Internet Technol. Secured Trans. (JITST) 1 (1/2) (2012). <http:// www.infonomics-society.org/JITST/ToUseorNottoUseMobileDevices.pdf>.
[4] I. Khalil, A. Khreishah, S. Bouktif, A. Ahmad, Security concerns in cloud computing, in: Proceedings of the 10th International Conference on Information Technology: New Generations, Las Vegas, Nevada, USA, April 15–17, 2013.
[5] http://www.digitalbuzzblog.com/infographic-2013-mobile-growthstatistics/ (accessed 10.01.14).
[6] I. Berni, B. Markelj, Blended threats to mobile devices on the rise, in: The International Conference on Information Society (i-Society), 2012, pp. 59–64.
[7] M. La Polla, F. Martinelli, D. Sgandurra, A survey on security for mobile devices, IEEE Commun.Surv.Tutorials 15 (1) (2013) (First Quarter).
[8]http://www.abiresearch.com/research/product/1012083-mobiledevice- security (accessed 10.01.14).
[9] M. Bishop, Computer Security: Art and Science, Addison-Wesley Professional, Reading, MA, 2002.
[10] M. Leandro, T. Nascimento, D. Santos, M. Westphall, C. Westphall, Multi-tenancy authorization system with federated identity for cloud-based environments using shibboleth, in: The Eleventh International Conference on Network (ICN), 2012, pp. 88–93.