State of the Art in Cloud Security

Vandana Birle[1] Prof. Abhishek Raghuvanshi[2]

Abstract— In this paper, we present an overview of existing cloud security algorithms. All these algorithms are described more or less on their own. Cloud security is a very popular task. We also explain the fundamentals of sequential rule mining. We describe today's approaches for cloud security. From the broad variety of efficient algorithms that have been developed we will compare the most important ones. We will systematize the algorithms and analyze their performance based on both their run time performance and theoretical considerations. Their strengths and weaknesses are also investigated. It turns out that the behavior of the algorithms is much more similar as to be expected.

I. INTRODUCTION

Cloud computing is a new computing paradigm that is built on virtualization, parallel and distributed computing, utility computing, and service-oriented architecture. In the last several years, cloud computing has emerged as one of the most influential paradigms in the IT industry, and has attracted extensive attention from both academia and industry. Cloud computing holds the promise of providing computing as the fifth utility after the other four utilities (water, gas, electricity, and telephone). The benefits of cloud computing include reduced costs and capital expenditures, increased operational efficiencies, scalability, flexibility, immediate time to market, and so on. Different service-oriented cloud computing models have been proposed, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Numerous commercial cloud computing systems have been built at different levels, e.g., Amazon's EC2, Amazon's S3, and IBM's Blue Cloud are IaaS systems, while Google App Engine and Yahoo Pig are representative PaaS systems, and Google's App and Salesforce's Customer Relation Management (CRM) System belong to SaaS systems. With these cloud computing systems, on one hand, enterprise users no longer need to invest in hardware/software systems or hire IT professionals to maintain these IT systems, thus they save cost on IT infrastructure and human resources; on the other hand, computing utilities provided by cloud computing are being offered at a relatively low price in a pay-as-you-use style.

II. LITERATURE SURVEY

A. *Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility*

AUTHORS: Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg, Ivona Brandic

With the significant advances in Information and Communications Technology (ICT) over the last half century, there is an increasingly perceived vision that computing will one day be the 5th utility (after water, electricity, gas, and telephony). This computing utility, like all other four existing utilities, will provide the basic level of computing service that is considered essential to meet the everyday needs of the general community. To deliver this vision, a number of computing paradigms have been proposed, of which the latest one is known as Cloud computing. Hence, in this paper, we define Cloud computing and provide the architecture for creating Clouds with market-oriented resource allocation by leveraging technologies such as Virtual Machines (VMs). We also provide insights on market-based resource management strategies that encompass both customer-driven service management and computational risk management to sustain Service Level Agreement (SLA)-oriented resource allocation. In addition, we reveal our early thoughts on interconnecting Clouds for dynamically creating global Cloud exchanges and markets. Then, we present some representative Cloud platforms, especially those developed in industries, along with our current work towards realizing market-oriented resource allocation of Clouds as realized in Aneka enterprise Cloud technology. Furthermore, we highlight the difference between High Performance Computing (HPC) workload and Internet-based services workload. We also describe a meta-negotiation infrastructure to establish global Cloud exchanges and markets, and illustrate a case study of harnessing 'Storage Clouds' for high performance content delivery. Finally, we conclude with the need for convergence of competing IT paradigms to deliver our 21st century vision.

B. *Methods and limitations of security policy reconciliation*

AUTHORS**:** MDaniel, P. ,Prakash, A.

A security policy is a means by which participant session requirements are specified. However, existing frameworks provide limited facilities for the automated reconciliation of participant policies. This paper considers the limits and methods of reconciliation in a general-purpose policy model. We identify an algorithm for efficient two-policy reconciliation, and show that, in the worst-case, reconciliation of three or more policies is intractable. Further, we suggest efficient heuristics for the detection and resolution of intractable reconciliation. Based upon the policy model, we describe the design and implementation of the Ismene policy language. The expressiveness of Ismene, and indirectly of our model, is demonstrated through the representation and exposition of policies supported by existing policy languages. We conclude with brief notes on the integration and enforcement of Ismene policy within the Antigone communication system.

C. *A unified scheme for resource protection in automated trust negotiation*

AUTHORS**:** Ting Yu , Winslett, M.

Automated trust negotiation is an approach to establishing trust between strangers through iterative disclosure of digital credentials. In automated trust negotiation, access control policies play a key role in protecting resources from unauthorized access. Unlike in traditional trust management systems, the access control policy for a resource is usually unknown to the party requesting access to the resource, when trust negotiation starts. The negotiating parties can rely on policy disclosures to learn each other's access control requirements. However a policy itself may also contain sensitive information. Disclosing policies' contents unconditionally may leak valuable business information or jeopardize individuals' privacy. In this paper we propose UniPro, a unified scheme to model protection of resources, including policies, in trust negotiation. UniPro improves on previous work by modeling policies as first-class resources, protecting them in the same way as other resources, providing fine-grained control over policy disclosure, and clearly distinguishing between policy disclosure and policy satisfaction, which gives users more flexibility in expressing their authorization requirements. We also show that UniPro can be used with practical negotiation strategies without jeopardizing autonomy in the choice of strategy, and present criteria under which negotiations using UniPro are guaranteed to succeed in establishing trust.

D. *Ciphertext-policy attributebased encryption*

AUTHORS: John Bethencourt, Amit Sahai, Brent Waters

In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute- Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we provide an implementation of our system and give performance measurements.

E. *Fuzzy identity based encryption*

AUTHORS**:** Amit Sahai , Brent R. Waters

We introduce a new type of Identity Based Encryption (IBE) scheme that we call Fuzzy Identity Based Encryption. A Fuzzy IBE scheme allows for a private key for an identity id to decrypt a ciphertext encrypted with another identity id # if and only if the identities id and id # are close to each other as measured by some metric (e.g. Hamming distance). A Fuzzy IBE scheme can be applied to enable encryption using biometric measurements as identities. The error-tolerance of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently contain some amount of noise during each measurement.

III. MORE TECHNIQUES

Attribute-Based Encryption (ABE) was first proposed by Sahai and Waters [22] with the name of Fuzzy Identity-Based Encryption, with the original goal of providing an error-tolerant identity-based encryption [23] scheme that uses biometric identities. In [24], Pirretti et al. proposed an efficient construction of ABE under the Random Oracle model and demonstrated its application in large-scale systems. Goyal et al. enhanced the original ABE scheme by embedding a monotone access structure into user secret key. The scheme proposed by Goyal et al. is called Key-Policy Attribute-Based Encryption (KP-ABE) [25], a variant of ABE. In the same work, Goyal et al. also proposed the concept of Ciphertext-Policy AttributeBased Encryption (CP-ABE) without presenting a concrete construction. CP-ABE is viewed as another variant of ABE in which ciphertexts are associated with an access structure. Both KP-ABE and CP-ABE are able to enforce general access policies that can be described by a monotone access structure. In [26], Ostrovsky et al. proposed an enhanced KP-ABE scheme which supports non-monotone access structures. Chase [27] enhanced Sahai-Waters ABE scheme and Goyal et al. KP-ABE scheme by supporting multiple authority. Further enhancements to multi-authority ABE can be found. Bethencourt et al. [28] proposed the first CP-ABE construction with security under the Generic Group model. In [29], Cheung et al. presented a CCA-secure CP-ABE construction under the Decisional Bilinear Diffie-Hellman (DBDH) assumption. In [29], the CCAsecure scheme just supports AND gates in the access structure. Towards proposing a provably secure CP-ABE scheme supporting general access structure, Goyal et al. [31] proposed a CP-ABE construction with an exponential complexity which can just be viewed as theoretic feasibility. For the same goal, Waters [30] proposed another CP-ABE scheme under various security assumptions. Aside from providing basic functionalities for ABE, there are also many works proposed to provide better security/privacy protection for ABE. These works include CP-ABE with hidden policy, ABE with user accountability [32], ABE with attribute hierarchy [33] and etc

In this paper, we surveyed the list of existing cloud security techniques. In a forthcoming paper, we pursue the development of a novel algorithm that efficiently mines sequential association rules from a market basket data set.

REFERENCES

[1] R. Buyya, C. ShinYeo, J. Broberg, and I. Brandic, “Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility,” Future Generation Comput. Syst., vol. 25, pp. 599–616, 2009.
[2] Amazon Elastic Compute Cloud (Amazon EC2) [Online]. Available: http://aws.amazon.com/ec2/
[3] Amazon Web Services (AWS) [Online]. Available: https://s3.amazonaws. com/

[4] R. Martin, "IBM brings cloud computing to earth with massive new data centers," InformationWeek Aug. 2008 [Online]. Available: http:// www.informationweek.com/news/hardware/data_centers/209901523
[5] Google App Engine [Online]. Available: http://code.google.com/appengine/
[6] K. Barlow and J. Lane, "Like technology from an advanced alien culture: Google apps for education at ASU," in Proc. ACM SIGUCCSUser Services Conf., Orlando, FL, 2007.
[7] B. Barbara, "Salesforce.com: Raising the level of networking," Inf.Today, vol. 27, pp. 45–45, 2010.
[8] J. Bell, Hosting EnterpriseData in the Cloud—Part 9: InvestmentValue Zetta, Tech. Rep., 2010.
[9] .A. Ross, "Technical perspective: A chilly sense of security," Commun.ACM, vol. 52, pp. 90–90, 2009.
[10] D. E. Bell and L. J. LaPadula, Secure Computer Systems: Unified Exposition and Multics Interpretation The MITRE Corporation, Tech. Rep., 1976.
[11] K. J. Biba, Integrity Considerations for Secure Computer Sytems The MITRE Corporation, Tech. Rep., 1977.
[12] H. Harney, A. Colgrove, and P. D. McDaniel, "Principles of policy in secure groups," in Proc. NDSS, San Diego, CA, 2001.
[13] P. D. McDaniel and A. Prakash, "Methods and limitations of security policy reconciliation," in Proc. IEEE Symp. Security and Privacy, Berkeley, CA, 2002.
[14] T. Yu and M. Winslett, "A unified scheme for resource protection in automated trust negotiation," in Proc. IEEE Symp. Security and Privacy, Berkeley, CA, 2003.
[15] J. Li, N. Li, and W. H. Winsborough, "Automated trust negotiation using cryptographic credentials," in Proc. ACM Conf. Computer and Communications Security (CCS), Alexandria, VA, 2005.
[16] Goyal, O. Pandey, A. Sahai, and B.Waters, "Attibute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Alexandria, VA, 2006.
[17] S. Yu, C. Wang, K. Ren, and W. Lou, "Achiving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE INFOCOM 2010, 2010, pp. 534–542.
[18] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp. Security and Privacy, Oakland, CA, 2007.
[19] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: .A practically motivated enhancement to attribute-based encryption," in Proc. ESORICS, Saint Malo, France, 2009.
[20] .A. Sahai and B. Waters, "Fuzzy identity based encryption," in Proc. Acvances in Cryptology—Eurocrypt, 2005, vol. 3494, LNCS, pp. 457–473.
[21] G.Wang, Q. Liu, and J.Wu, "Hierachical attibute-based encryption for fine-grained access control in cloud storage services," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Chicago, IL, 2010.
[22] .A. Sahai and B. Waters. Fuzzy Identity-Based Encryption. In Proc. of EUROCRYPT'05, Aarhus, Denmark, 2005.
[23] D. Boneh and M. Franklin. Identity-Based Encryption from The Weil Pairing. In Proc. of CRYPTO'01, Santa Barbara, California, USA, 2001.
[24] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure .Atrribute-Based Systems. In Proc. of CCS'06, New York, NY, USA, 2006.
[25] Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data. In Proc. of CCS'06, Alexandria, Virginia, USA, 2006.
[26] R. Ostrovsky, A. Sahai, and B. Waters. "Attribute-based encryption with
[27] non-monotonic access structures". In Proc. of CCS'06, New York, NY, 2007.
[28] M. Chase. "Multi-authority attribute based encryption". In Proc. of TCC'07,
[29] Amsterdam, Netherlands, 2007