INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

ISSN: 2454-9924

Contributory Broadcast Encryption with Efficient Encryption and Short Cipher texts

K ARUNA SUDHA[1], S.SURESH[2]

[1]M.Tech Student, Sree Rama institute of technology and science

Kuppenakuntla,Penuballi,Khammam,TS INDIA

[2]Asst Prof,CSE DeptSree Rama institute of technology and science
Kuppenakuntla,Penuballi,Khammam,TS INDIA

ABSTRACT:

Traditional broadcast encryption (BE) schemes allow a sender to securely broadcast to any subset of members but require a trusted party to distribute decryption keys. Group key agreement (GKA) protocols enable a group of members to negotiate a common encryption key via open networks so that only the group members can decrypt the ciphertexts encrypted under the shared encryption key, but a sender cannot exclude any particular member from decrypting the ciphertexts. In this paper, we bridge these two notions with a hybrid primitive referred to as contributory broadcast encryption (ConBE). In this new primitive, a group of members negotiate a common public encryption key while each member holds a decryption key. A sender seeing the public group encryption key can limit the decryption to a subset of members of his choice. Following this model, we propose a ConBE scheme with short ciphertexts. The scheme is proven to be fully collusion-resistant under the decision n-Bilinear Diffie-Hellman Exponentiation (BDHE) assumption in the standard model. Of independent interest, we present a new BE scheme that is aggregatable. The aggregatability property is shown to be useful to construct advanced protocols.

Index Terms—Cloud computing, Internet of Things (IoT), mixed negotiation approach, Quality of Service (QoS).

INTRODUCTION:

I NTERNET OF THINGS (IoT) is expected to be a worldwide network of interconnected objects [7]. IoT allows objects like computers, sensors, mobile phones, etc. to communicate via the Internet. It is characterized by limited capacities and constrained devices, and its development depends on new technologies including cloud computing. IoT can benefit from the unlimited capabilities and resources of cloud computing. Also, when coupled with IoT, cloud computing can in turn deal with real world things in a more distributed and dynamic manner. In this sense, IoT and cloud computing can complement each other. Cloud services are Internet-based IT services. Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are three representative examples.Compared with other models, cloud services are easier to access and use, cost-efficient, and environmentally sustainable. As they eliminate large upfront expenses in hardware and expensive labor costs for maintenance, cloud services are beneficial to small- and medium-sized enterprises. Moreover, large-sized enterprises with computationally intensive tasks can obtain results quickly, since their applications can scale up promptly. As the cloud market becomes more open and competitive, Quality of Service (QoS) will be more important. However, cloud providers and cloud consumers have different and sometimes opposite preferences. For example, a cloud consumer usually prefers a high reliability, whereas a cloud provider may only guarantee a less than maximum reliability in order to reduce costs and maximize profits. If such a conflict occurs, a Service Level Agreement (SLA) cannot be reached without negotiation. Automated negotiation occurs, when software agents negotiate on behalf of their human counterparts. It has been studied in electronic commerce and artificial intelligence for many years and is considered as the most flexible approach to procure products and services.

Existing System:

IoT allows connected objects to communicate via the Internet, whereas cloud computing promises unlimited resources delivered over the Internet. Zhou et al. review the

ISSN: 2454-9924

state of the art of integrating IoT and cloud computing and propose a cloud-based IoT platform to facilitate things application development. In conducting service research, many ideas and methods have been proposed . QoS is important in discovering, selecting, and composing Web services , grid services and cloud services. Li et al. report that commercial cloud services are not yet stable and ask for more attention to the performance, reliability, scalability, and security issues of cloud services. Wang et al. argue that QoS and SLAs are increasingly emphasized in enterprise cloud services, and automated SLA and adaptive resource management are needed. Automated negotiation occurs when software agents negotiate on behalf of their human counterparts. It has been studied in artificial intelligence and electronic commerce for many years . Jennings et al. argue that negotiation is the most fundamental mechanism to manage runtime dependencies among agents, and thus underpins cooperation and coordination.Lomuscio et al. argue that automated negotiation underpins the next generation of electronic commerce systems, and develop a classification scheme for negotiation in electronic commerce. It offers a systematic basis on which different negotiation mechanisms can be compared and contrasted.

Proposed System:

Internet startups are able to reside on a cloud to build their services even without their own infrastructure. A storage cloud allows users to store their data in data centers without worrying about backup, such that they can focus on their core businesses Amazon Simple Storage Service (Amazon S3), Microsoft Windows Azure Blob Storage (Azure Blob), and Aliyun Open Storage Service (Aliyun OSS) are three well-known storage clouds .Here, we present a motivating example, where a Storage

Consumer (SC) negotiates over QoS with a Storage Provider (SP). It contains conflicts that cannot be resolved without negotiation. Suppose that, five attributes, i.e., Availability (AVAL), Reliability (REL), Responsiveness (RESP), Security (SECY), and Elasticity (ELAS), are used to describe a storage cloud, as shown in Table I. The numbers are built upon our experiences with real-world storage clouds . Refer to for the definitions and the metrics of the five attributes. It is also shown in Table I that for the SC, availability is a higher-is-better attribute, for which a symbol is assigned beside its preferred values. By contrast, for the SP, availability is a lower-is-better one, for which a symbol is assigned beside its preferred values. However, the two parties differ in their preferences over availability. The SP puts a weight of 0.20 on availability, whereas the SC places a weight of 0.10 on it. For conciseness, we list corresponding numbers for other attributes in Table I, without going into details.

MULTI-ATTRIBUTE BILATERAL NEGOTIATION

Here, we introduce multi-attribute bilateral negotiations, with a focus on their negotiation protocol and negotiation strategies. In bilateral negotiations, two agents have a common interest in cooperation, but have conflicting interests regarding the particular way of doing so . In multi-attribute negotiations, multiple issues are negotiated among agents, where a win–win solution is possible. However, a multi-attribute negotiation is more complex and challenging than a single-attribute one, because of complex preferences over multiple issues and the multiple-dimensional solution space. For multi-attribute bilateral negotiations, which we deal with in the paper, their negotiation protocol and negotiation strategies merit special attention .

Negotiation Protocol

A negotiation protocol specifies the “rules of encounter” among agents . In this paper, we adopt an alternating-offers protocol for cloud service negotiation . In multi attribute bilateral negotiations, two agents alternately exchangetheir proposals and counter proposals, until one of them accepts a proposal, a failure to reach an agreement happens, or the deadline is reached. If the first case occurs, the negotiation ends successfully with an agreement established; otherwise, it fails and terminates with no deal made.

Negotiation Strategies

Once the negotiation protocol is chosen, negotiation strategies become critical. Two negotiation strategies, concession and tradeoff , can be used to make a proposal. When the deadline approaches or something undesirable happens, a party has to concede in order to make a deal. With a concession strategy, the party gradually reduces its utility until all conflicts are resolved.

ISSN: 2454-9924

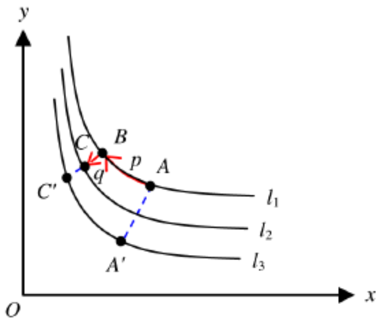

Fig. 1. Mixed negotiation approach.

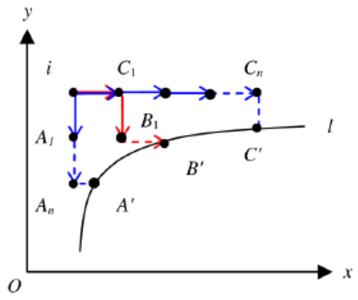

Fig. 2. Agent i's mixed behavior.

EVALUATION AND ANALYSIS

We conduct extensive simulations to evaluate the mixed approach for cloud service negotiation. First, we describe the experimental setup. Next, we describe the parameter setup. Finally, we report and analyze simulation results.

A. Experimental Setup

All simulations are conducted on a Lenovo Think Centre desktop with a 2.80-GHz Intel Pentium Dual-Core CPU and a 2.96-GB RAM, running Microsoft Windows 7 Professional Operating System. The simulations are implemented with Java under Net Beans IDE 7.2.1 with JDK 7u13. An alternating-offers protocol is adopted as the negotiation protocol, and a mixed negotiation strategy is compared with concession and tradeoff strategies. The negotiation process works as follows. First, without loss of generality, a SP sends its initial proposal to a SC. Next, if the proposal is accepted by the SC, negotiation ends successfully; otherwise, the SC uses either mixed, tradeoff, or concession negotiation approach to create a counter proposal. After that, the SC sends back the counter proposal to the SP, and the negotiation process repeats. The process ends once a proposal or a counter proposal is accepted, and it fails if no proposal is acceptable to both parties.

Java multithreading, which allows multiple tasks in a program to be executed concurrently, is the ideal technique to simulate the negotiation process. A thread is the flow of execution, from beginning to end, of

CONCLUSION

In this paper, we formalized the ConBE primitive. In ConBE, anyone can send secret messages to any subset of the group members, and the system does not require a trusted key server. Neither the change of the sender nor the dynamic choice of the intended receivers require extra rounds to negotiate group encryption/decryption keys. Following the ConBE model, we instantiated an efficient ConBE scheme that is secure in the standard model. As a versatile cryptographic primitive, our novel ConBE notion opens a new avenue to establish secure broadcast channels and can be expected to secure numerous emerging distributed computation applications

REFERENCES:

[1] M. Armbrust et al., “A view of cloud computing,” Commun. ACM, vol. 40, no. 4, pp. 50–58, 2010.

[2] D. Besanko and R. R. Braeutigam, Microeconomics, 3rd ed. Hoboken, NJ, USA: Wiley, 2008.

[3] Q. Duan, Y. Yan, and A. V. Vasilakos, “A survey on serivce-oriented network virtualizaiton toward convergence of networking and cloud computing,” IEEE Trans. Netw. Service Manag., vol. 9, no. 4, pp. 373–392, Dec. 2012.

[4] P. Faratin, C. Sierra, and N. Jennings, “Negotiation decision functions for autonomous agents,” Robot. Auton. Syst., vol. 24, no. 3-4, pp. 159–182, 1997.

[5] N. R. Jennings et al., “Automated negotiation: Prospects, methods and challenges,” Group Decis. Negotiation, vol. 10, no. 2, pp. 199–215, 2001.

[6] K. Leyton-Brown and Y. Shoham, Essentials of Game Theory: A Concise,

Multidisciplinary Introduction. San Rafael, CA, USA: Morgan & Claypool, 2008.

\[7] Q. Li et al., “Applications integration in a hybrid cloud computing environment: Modelling and platform,” Enterpr. Inf. Syst., vol. 7, no. 3, pp. 237–271, 2013.

[8] S. Li et al., “Integration of hybrid wireless networks in cloud services oriented enterprise information systems,” Enterpr. Inf. Syst., vol. 6, no. 2, pp. 165–187, 2012.

[9] S. Li, L. Xu, and X. Wang, “Compressed sensing signal and data acquisition in wireless sensor networks and Internet of things,” IEEE Trans. Ind. Informat., vol. 9, no. 4, pp. 2177–2186, Nov. 2013.

[10] A. R. Lomuscio, M. Wooldridge, and N. R. Jennings, “A classification scheme for negotiation in electronic commerce,” Group Decis. Negotiation, vol. 12, no. 1, pp. 31–56, 2003.

[11] J. F. Nash, “Equilibrium points in n-person games,” in Proc. Natl. Acad. Sci., vol. 36, 1950, pp. 48–49.

[12] D. Paulraj, S. Swamynathan, and M. Madhaiyan, “Process model-based atomic service discovery and composition of composite semantic web services using web ontology language for services (OWL-S),” Enterpr. Inf. Syst., vol. 6, no. 4, pp. 445–471, 2012.

[13] H. Raiffa, The Art and Science of Negotiation. Cambridge, MA, USA:

Harvard Univ. Press, 1982, pp. 148–165.

[14] L. Ren et al., “A methodology towards virtualisation-based high performance simulation platform supporting multidisciplinary design of complex products,” Enterpr. Inf. Syst., vol. 6, no. 3, pp. 267–290, 2012.

[15] A. Rubinstein, “Perfect equilibrium in a bargaining model,” Econometrica, vol. 50, no. 1, pp. 97–110, 1982.

[16] K. M. Sim, “Agent-based cloud computing,” IEEE Trans. Serv. Comput., vol. 5, no. 4, pp. 564–577, Nov. 2012.

[17] V. Stantchev and C. Schröpfer, “Negotiating and enforcing QoS and SLAs in grid and cloud computing,” in Proc. 4th Int. Conf. Grid Pervasive Comput., LNCS 5529. Geneva, Switzerland, 2009, pp. 25–35.

[18] F. Tao et al., “Research on manufacturing grid resource service optimalselection and composition framework,” Enterpr. Inf. Syst., vol. 6, no. 2, pp. 237–264, 2012.

[19] F. Tao et al., “Modelling of combinable relationship-based composition service network and the theoretical proof of its scale-free characteristics,” Enterpr. Inf. Syst., vol. 6, no. 4,, pp. 373–404, 2012.

[20] F. Tao et al., “FC-PACO-RM: A parallel method for service composition optimal-selection in cloud manufacturing system,” IEEE Trans. Ind.

Informat., vol. 9, no. 4, pp. 2023–2033, Nov. 2013.

K ARUNA SUDHA is an M.Tech Department of Co mputer Science & Engineering, Sreerama Institute of Technology & science, Penuballi Mandal, Khammam, Kotha Kuppenkuntla.

S. Suresh well known author and excellent teacher. He belongs to Computer Science &

Engineering. He is working as Vice Principal in Sree Rama Institute of Technology & Science, Kuppenakuntla, Penuballi, Khammam. He has vast teaching experience in various engineering colleges. To his credit couple of publications both National& International conferences / journals. His area of Interest includes Data Warehouse and Data Mining, information security, Data Communications &Networks, Software Engineering and other advances in Computer Applications. He has guided many projects for Engineering Students

ISSN: 2454-9924