INTERNATIONAL JOURNAL OF
RESEARCH IN COMPUTER
APPLICATIONS AND ROBOTICS
ISSN 2320-7345

SURVEY ON SECURE PROTOCOLS FOR KEY EXCHANGES IN DATA-INTENSIVE APPLICATIONS OVER CLOUD COMPUTING

Merlin Shirly T[1], Margret Johnson[2]

[1]PG Full Time Student, CSE Department, Karunya University, Coimbatore

[2]Assistant Professor, CSE Department, Karunya University, Coimbatore

[1]merlinshirly@gmail.com, [2]margret_cse@karunya.edu

Abstract

In order to run data-intensive applications, the users can use hybrid environment such as cloud computing instead of purchasing their own computing infrastructure. Cloud computing provides vast storage for data-intensive application and also provides computation capabilities. During the scheduling of these data-intensive applications, the data flows between the controller and the server instances while scheduling. During the flow of data between the server instances, the data may be stolen or modified by malicious parties due to the less security in hybrid cloud system. In order to acquire security, the data are encrypted before sent to the cloud storage for storing. The data are encrypted and the session keys are calculated by the cloud controller and server instances. The private keys had to be exchanged between the cloud controller and server instances in a secure manner. Before sending the data from the cloud controller to server instances, they need to authenticate themselves. This authentication has to be done in order to identify and remove the malicious participants. There are different protocols available for authenticating the users in the communication. In order to authenticate the cloud users involved in communication, the secure protocols are used. Those secure protocols are used for providing security in key exchange between cloud controller and server instances. The secure protocols differ in efficiency in terms of number of rounds involved in authentication and the flexibility of users in joining the cloud network.

.

Keywords: Cloud Computing, hybrid environment, Private Keys, Authentication, Data-Intensive.

1. Introduction

The Cloud computing includes the usage of computing resources such as hardware and software. These resources are delivered as the service over the network. Now-a-days the principles of emerging cloud computing are attractive and also provides technical and financial advantages [12]. Now-a-days the new technologies and services are used in cloud computing infrastructures. Security is one of the main critical aspects in cloud computing because the sensitive and importance of data stored in cloud. It also has several other major issues such as data security, trust and performance issues. But the cloud infrastructures are very useful for business and it is very economical too.

One of the issues is the management of data that might not be fully trustworthy because it involves the risk of malicious insiders. The other major problems are preserving confidentiality and integrity of data in providing data security. Confidentiality is the prevention of disclosure of information. The main method used for preserving data confidentiality is data encryption [12]. The initial solution to provide data security is obtained by encrypting the data stored in cloud. Encryption seems like the perfect solution for ensuring data security however it has its own drawbacks. Encryption of data – intensive data generally takes larger time.

Data splitting is generally faster than encryption. The data splitting technique is to split data over multiple hosts that communicate with each other [12]. The user alone can access both the hosts and they can alone collect and combine the datasets to create the original data. This method is extremely faster, but it needs at least two separate homogeneous service providers.

Other issues in cloud computing includes Trust, Authenticity (Integrity and Completeness) and legal issues. The trust between the customer and the services provider is the major issues among many others [13]. Service Level Agreement (SLA) is the legal document between the customers and the service providers. . This document contains the agreements between the customer and the service providers. The legal issues include several regulatory requirements, privacy laws and data security laws that the cloud systems needs to adhere to. The laws vary from country to country therefore the users have no control over the physical location of data.

Cloud computing technology offers the following advantages: 1. Unlimited storage with pay-as-you-go mode, 2. Collaboration among the users by enabling online sharing of applications and information, 3. Portability (i.e. the cloud users can access their data from anywhere), 4. Better reliability and security (i.e. there is no need for the user to worry about their hardware failure or hardware being stolen). 5. Reduction in operation cost (i.e. no need of paying wages for expert staff) [13]. 6. Scalability [13]. 7. Backup and Recovery: In certain cases the cloud itself acts as a backup repository for the data. 8. Redundancy, 9. Increase in storage capacity. 10. Diversity in device location and location independency [14]. The cloud services are very useful but have their own demerits.

2. Related Works

The survey is done on the following secure protocols for secure Key Exchange and the methodologies used are identified and the merits are listed below.

2.1 Authenticated Group Key Exchange Protocol

The Authenticated Group Key Exchange protocol uses a scalable compiler that transforms any Group Key Exchange protocol secure. The compiler constructs the protocols as follows. The Scalable Compiler used in [1] transforms any group key exchange protocol that provides secure against the passive eavesdropper. It is secure against an adversary who controls all the communication in the network. In initialization phase, verification keys are generated. Then message is broadcasted by each user. After receiving the message, signature is verified. By using the protocol used in [1], the number of rounds in modular exponentiations per user is reduced.

The advantages of the protocol used in [1] are as follows. This scalable compiler uses constant number of rounds. It requires only O(1) modular exponentiations per user. It also achieves forward secrecy. in that particular subsection.

2.2 Dynamic Group Diffie - Hellman Key Exchange

The Dynamic Group Diffie – Hellman Key Exchange in [2] uses a protocol named as Authenticated Key Exchange, AKE^{+}. It provides security against strong corruption. The AKE^{+} protocol used in [2] is the combination of decisional Diffie-Hellman problem and the pseudo-random function. The protocol proposed in [2] is used to incorporate major missing details such as Strong-Corruption and concurrent execution of protocols to the group Diffie-Hellman Key Exchange. This protocol consists of Setup1^{+}, Remove1^{+} and Join1^{+} algorithms for dynamically initializing, adding and removing the parties [2]. This protocol avoids the missing of concurrent session execution and also avoids strong corruption.

The merits are as follows. The execution of the protocol is provably secure. It provides better security guarantees. It allows concurrent execution between the parties and it also achieves forward secrecy.

2.3 Password - Based Authenticated Key Exchange

The Password – Based Authenticated Key Exchange protocol in [3] uses (Chosen Plaintext Attack) CPA secure encryption with an associated hash function, (Chosen Cipher text Attack) CCA secure encryption scheme. The algorithm in [3] is used to overcome the insecurity in off-line dictionary attacks. By using the method in [3], a new approach is proposed.

The approach used in [3] provides the following merits. It guarantees mutual authentication and also automatically handles arbitrary password distribution

.

2.4 One Round Protocol for Tripartite Diffie – Hellman

The One Round Protocol consists of non -interactive Pubic Key System. This protocol that is used in [4], overcomes the cumbersome in terms of number of rounds. The protocol in [4] proposed a non-interactive Public-Key System, that does not need participants to be connected at that same time and it uses Diffie-Hellman for key exchange.

The merits of using the protocol in [4] are as follows. It does not need participants to be connected at the same time. The design of the protocol in [4] is simple also minimizes the number of rounds in communication to one. But the protocol in [4] lacks in authentication. This protocol allows man in middle attack [4].

2.5 Authenticated Multi-Party Key Agreement Protocol

The Multi-Party Key Agreement in [5] uses the following methodologies. They are Key Agreement protocol based on Diffie-Hellman that uses public key techniques, Diffie-Hellman computation for Key Confirmation and Key Establishment protocol. The protocol in [5] is used to design Key Agreement protocol that authentication for multi-party.

A multi-part scheme in [5] based on the specified 2-party scheme. This scheme used in [5] reduces the number of rounds required for key computation.

2.6 Authenticated Group Key Agreement Protocol

The Authenticated Group Key Agreement uses Two-Party Key Exchange Protocol. In [6], authors design the authenticated key agreement protocol to provide Perfect Forward Secrecy (PFS), resistance to known-key attacks, key authentication, key integrity and Key Confirmation. The paper [6] aims to provide resistance against adversaries, integrity, and authentication in key calculation. The Authenticated protocol provides perfect forward secrecy. (i.e. resistant to know Key Exchange Protocol).

The protocol in [6] provides resistance to active adversaries. The shared keys in [6] are long-term secret keys and it provides Perfect Forward secrecy.

2.7 Key Agreement in Dynamic Peer Group

The methodology used in [7] is CLIQUES protocol suite that is formed by two Initial Key Agreement (IKA) protocols. IKA 1: It consists of an up flow and down flow stages [7]. The purpose of up flow is to collect contributors from all group members one per round. IKA 2: Achieves complete policy independency.

The protocol in [7] is simple and straight forward. By using Internet Key Authentication (IKA), the amount of computation performed by each group member is minimized. It also provides Authenticated Key Exchange and Mutual Authentication. But the protocol in [7] does not provide fault-tolerant in the presence of malicious fault inside a group and it does not recognize multiple players' instance. So, the adversary may activate in concurrent and simultaneous session.

2.8 Secure Fault-Tolerant Conference-Key Agreement Protocol

The methodologies used in [8] are Diffie-Hellman Key Exchange, Conference-Key Agreement and Conference-Key Distribution. The broadcast channels are authenticated by these methodologies in order to escape from the possible attacks from impersonators. The protocol in used by [8], prevents a passive adversary from getting information about the Conference Key established by the honest participants. It also allows the honest participants to agree on common Conference Key despite of how many participants are malicious.

Protocol used in [8] is round-efficient. It uses only two rounds to compute a common conference key after all malicious participants are detected. This protocol is message - efficient. The size of the messages sends by participants is proportional to the number of participants.

2.9 Provably Authenticated Group Diffie – Hellman Key Exchange - The Dynamic Case

The scheme proposed by [9] consists of Key Generation Algorithm where session keys are generated, Key Setup Algorithm, Key Remove Algorithm, and Key Join Algorithm. This approach in [9] ensures security in existing system. In [9] authors design an Authenticated Key Exchange protocol that works in a scenario where the group membership is not known in advance and parties may join and leave the multicast group at any given time. It also aims at achieving message confidentiality and data integrity in multi-cast messages.

The merits of [9] are as follows. There is no need to know the membership in advance [9]. Therefore the parties are allowed to join and leave the multi-cast group at any time. It provides Authenticated Key Exchange and mutual Authentication. It does not recognize multiple players' instance. So, the adversary may activate in concurrent and simultaneous session.

2.10 Multi-Recipient Public-Key Encryption

The aim of [10] is to construct an n-recipient scheme to have "shortened cipher text". The cipher text length is almost half. The method used in [10] ensures security and the reduction of the length of the cipher text. The methodologies used in [10] are RSA algorithm along with single-recipient scheme. It includes Key Generation Algorithm, Key Encryption Algorithm and Key Decryption Algorithm.

The merits of [10] are as follows. The length of the cipher text is almost half of the trivial scheme. Encryption operation is significantly faster. This scheme is secure against chosen plaintext attack. Extra cost is required for each recipient cipher text.

2.11 Efficient Password-Authenticated Key Exchange

The approach used in [11] finds an efficient solution to the off-line dictionary attacks. It uses Diffie-Hellman assumption. The methodologies used are Diffie – Hellman Algorithm for key exchange and Authenticated Key Exchange for authenticating the generated keys

The merits of the exchange used in [11] are as follows. This protocol requires only three rounds. It does not require public key. So, it avoids problem with Public Key Infrastructure such as revocation, Key Management issues. It also provides forward security. But, the adversary may succeed by guessing which distribution was chosen.

3. Conclusion

In this paper, we presented a survey in the secure protocols for communication. We reviewed several protocols for secure key exchange and to provide authentication. Our analysis made it clear there is no unique solution for achieving all the requirements. Security is achieved by using the above protocols. Round efficiency and message efficiencies are also achieved in [8] in addition to security, data integrity and confidentiality.

REFERENCES

[1] J. Katz, M. Yung, “Scalable Protocols for Authenticated Group Key Exchange”, Journal of Cryptology 20 (1), 2007, pp. 85-113

[2] E. Bresson, O. Chevassut, D. Pointcheval, “Dynamic Group Diffie-Hellman Key Exchange under Standard Assumptions”, Advances in Cryptology 2332, 2002, pp. 321-226

[3] A. Groce, J. Katz, “A new framework for efficient password-based authenticated key exchange”, in: Proceedings of the 17th ACM conference on Computer and communications security, New York, USA, 2010.

[4] A. Joux, “A One Round Protocol for Tripartite Diffie–Hellman”, Journal of Cryptology 17(4), 2004, pp. 263-276.

[5] M. Just, S. Vaudenay, “Authenticated multi-party key agreement“, in: Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security, London, UK, 1996, pp.36-49..

[6] H.K. Lee, H.S. Lee, Y.R. Lee, ”An Authenticated Group Key Agreement Protocol on Braid Groups”, IACR Cryptology ePrint Archive, 2003.

[7] M. Steiner, G. Tsudi, M. Waidner, “Key agreement in dynamic peer groups“, IEEE Transactions on Parallel and Distributed Systems 11(8), 2000.

[8] W. G. Tzeng, “A Secure Fault-Tolerant Conference-Key Agreement Protocol”, IEEE Transactions on Computers 51(4), 2000.

[9] E. Bresson, O. Chevassut, D. Pointcheval, “Provably Authenticated Group Diffie-Hellman Key Exchange – The Dynamic Case”, Advances in Cryptology 2248, 2001, pp. 290-309.

[10] Kaoru Kurosawa, “Multi-recipient Public-Key Encryption with Shortened Ciphertext”, in: Proceedings of the 5th International Workshop on Practice and Theory in Public Key Cryptosystems: Public Key Cryptography, London, UK, 2002, pp. 48-63.

[11] J. Katz, R. Ostrovsky, M. Yung, ”Efficient Password-Authenticated Key Exchange using Human-Memorable Passwords”, in: Proceeding EUROCRYPT ’01 Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advance in Cryptology, London, UK, 2001 ,pp. 475-494.

[12] Cloud Computing Security Issues and Solutions. Available: http://cleverlogic.net/articles/cloud-computing-security-issues-and-solutions, accessed on 12 December 2013.

[13] Benefits of cloud computing. Available: http://www.business.qld.gov.au/business/running/technology-for-business/cloud-computing-business/cloud-computing -benefits, accessed on 12 December 2013.

[14] Cloud computing pros and cons. Available: http://www.javacodegeeks.com/2013/04/advantages-and-disadvantages-of-cloud-computing-cloud-computing-pros-and-cons.html, accessed on 12 December 2013.