Research Journal of Applied Sciences, Engineering and Technology 11(2): 144-149, 2015
DOI: 10.19026/rjaset.11.1700
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: March 19, 2015 Accepted: April 13, 2015 Published: September 15, 2015

Research Article

Ant Colony Based Authentication System for Cloud Computing

M. Hemanth Chakravarthy and E. Kannan
Department of Computer Science and Engineering, Vel Tech University, Chennai-62, Tamil Nadu, India

Abstract: In today's world key management for secured cloud is very essential. Dealing huge data on computing is one of the major requirement of the modern computing. This study proposes ant colony based authentication mechanism for cloud system. Ant Colony Optimization (ACO) is a swarm intelligence technique. ACO provides optimality in many discrete mathematical problems in almost all engineering problem domains. ACO follows the imitation of behavioral aspects of ant. Recent researchers highly following swarm intelligence algorithms for critical and real time problems. Secured cloud is an important research issue due to its variety of customers, devices used for access, variant parameters and metrics involved. The clouds are accessed by the modern hand held devices, so smaller sizes of security keys are much preferred for encryption algorithm. Further, few researchers improved the performance of RSA using Chinese Remainder Theorem. Even though, it is still a question for those approaching the clouds using their hand held systems in terms of processing time, memory and bandwidth.

Keywords: Ant colony optimization, cloud computing, cryptography, key management, security

INTRODUCTION

Cloud computing is a kind of high performance computing, which includes distributed computing, grid computing and cloud computing. The past technologies such as distributed computing and parallel computing are not highly suitable for the recent advancements because, the modern computer industry is operating very large amounts of data which is geographically, distributed. The emergence of cloud computing from distributed and grid computing will provide promise to save money by making it imperative for organizations.

The basic attributes of cloud computing are, availability, collaboration, elasticity, lower infrastructure, mobility, risk reduction, scalability, virtualization and computational risk to implement cloud computing. Cryptography is one of the important sciences in the current era, the importance of cryptography comes from the intensive digital transactions which we daily perform on the internet and other communication channels. Credential systems such as online trading, on line booking, on line transaction are major requirements for this modern generation. These applications required privacy infringement which becomes a major issue in the research of Internet security.

For the past few years, the cloud computing is one among top 10 growing technology, which proves a significant impact on IT in the future. However, there are lacks of security models, frameworks and certificates in cloud computing. ISO 27000 and NIST-FISMA provides cloud certificate in the recent days. These cloud security certificates help cloud providers to improve the consumers trust. Even though, these standards are still lacking from covering the full complexity of the cloud computing model.

In the world of cloud computing, there are lacks of compliance to standards, reporting, monitoring, service level agreements and legal acts. The providers have data-centres worldwide and customer can dynamically allocate their data among various data centres. Hence, this creates the customers anxiety because they may not know where their data is at any given time. Service providers and most governments have the ability to track and manage records. Most of these data will flow in and out of their environments. Here the major concern is the level of trust and transparency of the customer which should be well known to the customers through proper documents and policies, also the customers can test and identify their trust level at any point of time.

The biggest benefit of cloud computing is the centralization of data. Organizations have an issue with asset protection, in no small part because of data being stored in numerous places, like laptops and the desktop. Thick clients are apt to download files and maintain them on the hard drive and there are plenty of laptops out there with non-encrypted files. Using thin clients creates a better chance for centralized data storage. As such, there's less chance for data leakage. Centralization also provides the opportunity for better

Corresponding Author: M. Hemanth Chakravarthy, Department of Computer Science and Engineering, Vel Tech University, Chennai-62, Tamil Nadu, India

monitoring. That data is in one place makes it easier to check in on user data and verify that access.

The same security issues that the organization deals with are the sorts of issues that SaaS providers will faces the securing network, hardware issues, applications and data. But compliance adds another level of headache. Regulations like Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLBA) and industry standards like the Payment Card Industry Data Security Standard (PCI DSS) make things particularly challenging.

Private credentials offer authentication and authorization based on the attributes possessed by an user, rather than the identity of the user. They also satisfy properties such as unlink-ability, unforgeability, property sharing resistance, confidentiality and selective disclosure of attributes (Athavale *et al*., 2009). Defense messaging system takes a message and forwards it to the intending recipients or parties based on the message criteria for immediate action (Qing-Hai *et al*., 2012).

Data encryption is widely used to ensure security, the encryption function, source file is encoded using a special number or message. The value of this key modifies the detailed operation of the algorithm. That is, if the same data is encrypted using two different keys, the results will be totally dissimilar. Hence, the encryption algorithms and security keys are playing major role in cryptography and ACO can be used for their Key management.

LITERATURE REVIEW

QoS-oriented is also an important aspect in cloud computing. The availability of cloud computing resources is analyzed from QoS of a single cloud resource node. Wang *et al*. (2013) proposed QoS Oriented monitoring model, in which, a monitoring model of cloud computing, dynamic process of the cloud computing service, described by common attribution and special attribution to QoS of some cloud resources.

Zehua and Xuejie (2009) analyzed the security issues in the cloud computing, briefed about the Open Cloud Computing Federation (OCCF). Zehua and Xuejie (2009) proposed Mobile Agent Based Open Cloud Computing Federation (MABOCCF) mechanism. MABOCCF combines the mobile agent and cloud computing to provide a realization for the open cloud computing federation. MABOCCF offers multiple heterogeneous cloud computing platforms and realizes portability and interoperability.

Defining a framework is an initial process of the security model of cloud computing. A cloud security management framework is proposed by Almorsy *et al*. (2011). This framework is based on aligning the FISMA standard to fit with the cloud computing model. This framework is based on improving collaboration between cloud providers and service providers, which defined on top of a number of security standards.

Public-key encryption schemes are secure only if the authenticity of the public key is assured. A public-key certificate scheme provides the necessary security (William, 2005). A simple public-key algorithm is Diffie-Hellman key exchange this protocol enables two users to establish a secret key using a public-key scheme based on discrete logarithms. The protocol is secure only if the authenticity of the two participants can be established.

Implementation of cloud become more rapid in the recent years, such as Wu and Huang (2011), Mehdi *et al*. (2011), Kumar and Balasubramanie (2012) and Ponnuramu and Tamilselvan (2012). Wu and Huang (2011) implemented quasi-experimental method was applied to the study of 110 5th grade students of Tunglo Elementary School, Taiwan. Mehdi *et al*. (2011) proposes Impatient Task Mapping in Elastic Cloud using Genetic Algorithm. This algorithm finds a fast mapping using genetic algorithms. The genetic algorithm with "exist if satisfy" condition is speeding up the mapping process. The genetic algorithm is implemented using Cloud-sim.

Infrastructure as a Service (IaaS) is one among the cloud services that provides a computing resources for demand in various applications like Parallel Data processing. The computer resources offered in the cloud are extremely dynamic and probably heterogeneous. Nephele is the data processing framework used to exploit the dynamic resource allocation offered by IaaS clouds for task scheduling.

The quasi-experiment results showed that cloud computing was better than traditional IT system of educational environment. Cloud-sim simulator is a cloud benchmark which is used to test algorithms in cloud computing. Mapping time and make-span are the performance metrics in the cloud based mapping algorithms. Tasks scheduling and processing in cloud offers automatically instantiated and terminated job execution. The present methodologies are increases the efficacy of the scheduling algorithm for the real time Cloud Computing services. These Algorithms utilizes the Turn around Time which also assigns high priority for task of early completion and less priority for abortions/deadlines issues of real time tasks.

Wu and Huang (2011) recommended the cloud computing infrastructure to education in real world. The results of genetic algorithm in the cloud environment shows an improvement than MCT algorithm which also improves the throughput, hence can be used to map more jobs to cloud resources. The scheduling algorithms in cloud implemented on both preemptive and Non-preemptive methods. This method outperform, than the existing utility based scheduling algorithm on preemptive and Non-preemptive scheduling methods. Hence, a novel turn-around time utility scheduling approach with high priority and low priority tasks.

As early stated, the RSA is most widely used for a long time and it is well understood algorithm. In the other end, the hackers will crack the RSA which used

smaller keys. Hence, the size of key is increased from its initial version of 256 to 512-bits. Over time this further increased to 768, 1,024 and 2,048 bits, respectively. More recently, NIST recommended the combination of 128 bit AES keys with 3,072-bit RSA keys. Meanwhile, the European Committee are recommending 128 bit AES keys with 6,000-bit RSA keys.

The size of higher bits security key will increase the security of the algorithm but it is expensive in terms of computational requirements. For example, increasing from a 1,024-bit RSA key to a 2,048-bit key requires 8 times of the computations/processing. This is not recommended for hand-held products like Personal Digital Assistant (PDA) and communication devices, because it simply not having the processing capability to use RSA keys of 3,072 bits and higher (Brohi *et al*., 2014).

METHODOLOGY

ACO based authentication system for cloud computing: This study proposed ant colony based authentication mechanism for cloud system. Ant Colony Optimization (ACO) is a swarm intelligence technique. ACO provides optimality in many discrete mathematical problems in almost all engineering problem domains. ACO follows the imitation of behavioral aspects of ant. Recent researchers highly following swarm intelligence algorithms for critical and real time problems.

Attacks, may be passive attack or active attack, which will collapse the performance of the whole network. The attacks on cloud computing are much uncomplicated than other network as it used by many users at a time and at a various level. And most of the security issues in the cloud computing is only depends only to the user. Hence, designing a secured authentication against attracts is a critical task in cloud computing. As the security of cloud involves real time monitoring, this study proposes, an ant colony optimization as mobile agent and provides secured key/group management.

ACO algorithms take inspiration from the behavior of ants in nature. The classification and different kinds of IDS are shown in Fig. 1.

The main source of inspiration is found in the ability of certain types of ants, e.g., the family of Argentine ants, to find the shortest path between their nest and a food source using a volatile chemical substance called pheromone. Ants traveling between the nest and the food source leave traces of pheromone as they move. They also preferentially go in the direction of high pheromone intensities.

The proposed methodology and the security requirements of proposed Request based IDS are discussed in this section. For this extended IDS, ACO is used as Identification Agent (IA) and Target Agent (TA). In the initialization of network phase, ACO flooded in the network as IA to identify all authenticated members in order to process handshake. In the later stage, the ACO is used as TA for authenticating member and preventing non-member.

Hence, there are four components in the proposed system:

- **Member:** A member is an entity who belongs to the group. U∈G means that U belongs to the group G.
- **Non-member:** A non-member is an entity who does not belong to the group. U/∈ G means that U does not belong to the group G.
- ACO-IA is responsible for adding users into his group.
- ACO-TA is responsible for revealing users as well as checking whether handshake players belong to his own group.

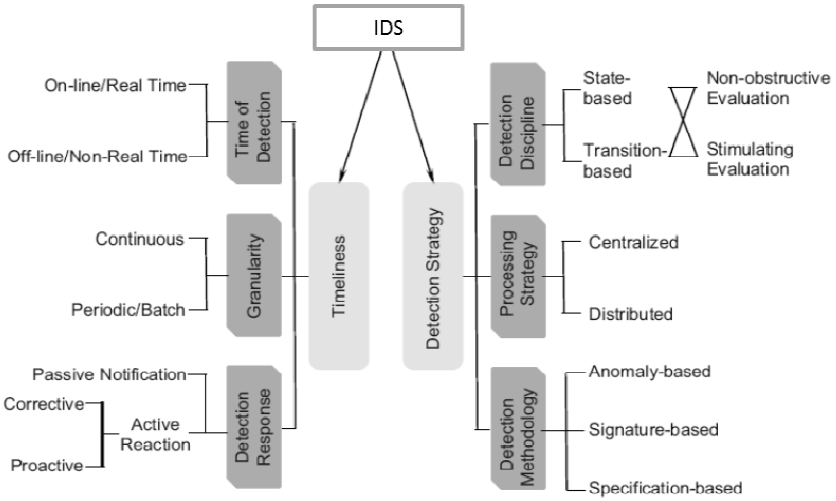

Fig. 1: Kinds of IDS

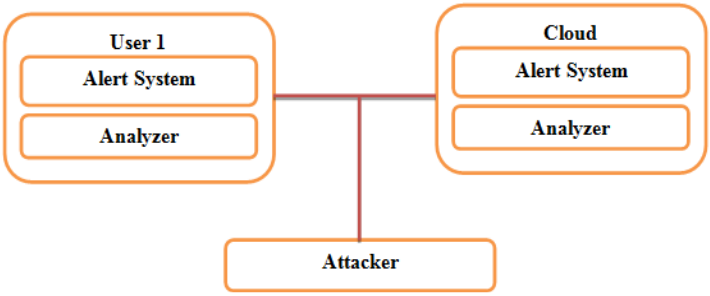

Fig. 2: System design of proposed mobile agent model

The implementation of this attractive scenario is explained hereunder.

Setup: The common parameter generation algorithm. Given a security parameter k, Setup outputs the public parameters (param) that are common to all groups.

KeyGen: The group public/secret key generation algorithm. KeyGen is run by ACO-IA and ACO-TA. Given param, KeyGen outputs a group public key gpk, a secret key of ACO-IAisk and a secret key of ACO-TAtsk.

Add: The member addition algorithm. Add is executed by a non-member A and ACO-IA. Given param, gpk and isk, Add outputs a membership certificate (certA), a secret key (skA) and ID of A (IDA).

Handshake: The authentication protocol executed between two players A and B, based on the public input param. The group public keys (gpkA and gpkB), certificates (certA, certB) and secret keys (skA, skB) of A and B are input to Handshake. The output of the algorithm is either rej or acc. A Handshake ←→ B means the situation in which A and B executes Handshake.

Group trace: A handshake player's group trace algorithm. Given gpk, tsk and a transcript TA, B, Group Trace outputs yes if A, B ∈ G; otherwise, Group Trace outputs no.

Request reveal: The handshake player tracing algorithm. Given gpk, tsk, certA, skA, a transcript TA, B and internal information that are used in Handshake by a player A, Request Reveal outputs the member B.

The proposed mobile agent based secured model is shown in Fig. 2. In each node, two types of systems are defined, such that Alert system and analyzer. The analyzer consists of mobile agent which is defined and used as program model to collect information regarding security information. The analyzer receives the security key and verifies the authentication. The alert system broadcast the alert messages to the authenticated neighbors when it identifies the intruder. This alert message also used for verification if the identified attacker may be authenticated user of other authenticated nodes of the concern node.

When an authenticated node of a group receives the message from unknown node, it initiates the mobile agent to collect security information of the unknown node. The MD5 hash function H is used to create message digest H (M) in the authenticated node. The authenticated node generates the following digital signature, if the unknown node is an authenticated node of the group:

$$d_{sign} = (H(M))^{d} \bmod n \quad (1)$$

The authenticated node is encrypting message by using its digital signature. Encrypting the message digest H (M) with its private key d where, n = p∗q, p and q are random prime numbers with p ≠ q. The source node forwards d_{sign} with data M, (d_{sign}, M) to its neighboring node through the path it takes to reach sink.

A neighboring node on reception of (d_{sign}, M) and the path in the data packet, verifies the digital signature by comparing decrypted value of d^{e}_{sign} mod n with message digest H (M). The d^{e}_{sign} mod n is key (e, n) using the formula, decrypted using sender's public key:

$$d^{e}_{sign} \bmod n = ((H(M))^{d} \bmod n)^{e} \bmod n \quad (2)$$

$$= (H(M))^{ea} \bmod n \quad (3)$$

By applying Little Fermat's Theorem to above Equation, it can be shown that:

$$d^{e}_{sign} \bmod n = H(M) \quad (4)$$

If the generated H (M) by the receiver and the decrypted H (M) of digital signature d^{sign} is equal, then the receiver accepts the data; otherwise rejects the data and informs the sender that the data is altered through by generating route error packet. This process is repeated in every hop of the node disjoint path between source and destination. The proposed public key crypto system provides authentication, integrity and non-repudiation in the ad hoc network.

Table 1: Simulation parameters

Parameters	Values
Simulation area	200×200 m^2
Propagation	Two ray ground
MAC type	802.11
Antenna	Omni antenna
Queue	Drop tail/priority
Queue limit	50
No of nodes	10 to 500
Packet type	CBR
Packet size	220 bits

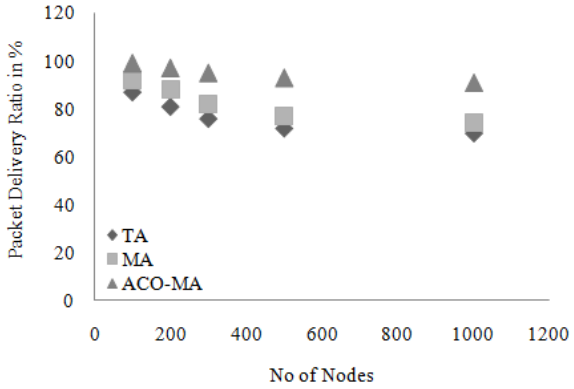

Fig. 3: Reliability when 10% of attacker node

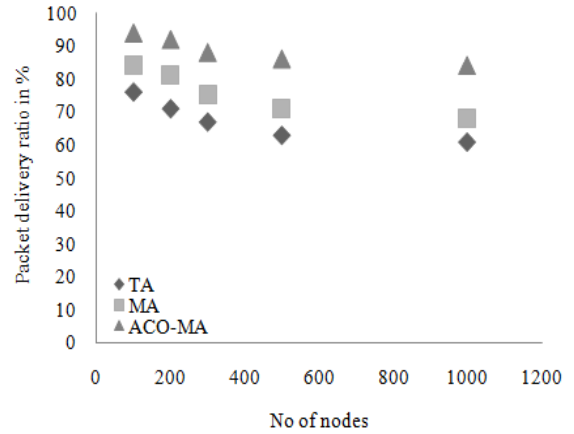

Fig. 4: Reliability when 20% of attacker node

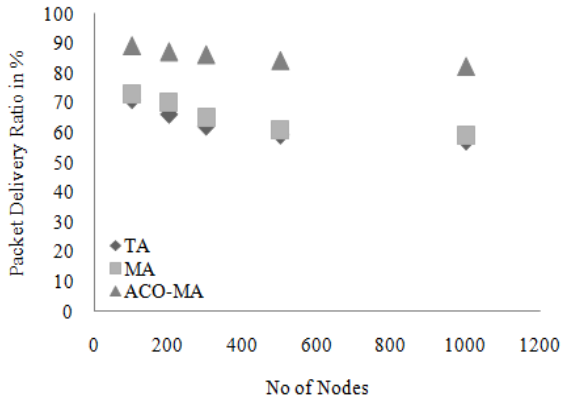

Fig. 5: Reliability when 30% of attacker node

RESULTS

The proposed study is simulated in NS2. The simulation parameters of the proposed study are shown in Table 1. The proposed study is compared with existing traditional Target Authority (TA) Model and Mobile Agent (MA) model. The Reliability and scalability are major research issues in the design of networking protocol. Hence, the proposed study are analyzed the reliability and scalability of proposed study and compared with TA and MA. The reliability is computed based on the simulation data and result. The number of node is varied and number of attacker node also varied for performance comparison.

The reliability is computed based on effective packet delivery, which analyzed on different test cases, test case 1: when 10% of attacker node, test case 2: 20% of attacker node and test case 3: 30% of attacker node are shown in Fig. 3 to 5.

CONCLUSION

The scalability is observed from the above data, in which the system has 70% and above packet delivery ratio only accepted as scalable system. Hence, when 10% attacker nodes are inserted (Fig. 3) the TA supports up to 500 Nodes, whereas MA and proposed ACO-MA support 1000 Nodes. When attacker nodes are increases to 20% (Fig. 4), the TA supports up to 200 Nodes only, whereas MA supports 500 Nodes and proposed ACO-MA support even for 1000 Nodes. Similarly, the TA and MA supports only 100 Nodes when 30% of attacker nodes are inserted (Fig. 5). The proposed system always supports above 80% packet delivery ratio. Hence, the proposed system proves better reliability and scalability than the existing systems.

REFERENCES

Almorsy, M., J. Grundy and A.S. Ibrahim, 2011. Collaboration-based cloud computing security management framework. Proceeding of the IEEE International Conference on Cloud Computing (CLOUD), pp: 364-371.

Athavale, A., K. Singh and S. Sood, 2009. Design of a private credentials scheme based on elliptic curve cryptography. Proceeding of the 1st International Conference on Computational Intelligence, Communication Systems and Networks (CICSYN'09), pp: 332-335.

Brohi, S.N., M.A. Bamiah, S. Chuprat and J.L.A. Manan, 2014. Design and implementation of a privacy preserved off-premises cloud storage. J. Comput. Sci., 10: 210-223.

Kumar, S.K.S. and P. Balasubramanie, 2012. Dynamic scheduling for cloud reliability using transportation problem. J. Comput. Sci., 8: 1615-1626.

Mehdi, N.A., A. Mamat, H. Ibrahim and S.K. Subramaniam, 2011. Impatient task mapping in elastic cloud using genetic algorithm. J. Comput. Sci., 7: 877-883.

Ponnuramu, V. and L. Tamilselvan, 2012. Data integrity proof and secure computation in cloud computing. J. Comput. Sci., 8: 1987-1995.

Qing-Hai, B., Z. Wen-Bo, J. Peng and L. Xu, 2012. Research on design principles of elliptic curve public key cryptography and its implementation. Proceeding of the International Conference on Computer Science and Service System (CSSS, 2012), pp: 1224-1227.

Wang, E.D., N. Wu and X. Li, 2013. QoS-oriented monitoring model of cloud computing resources availability. Proceeding of the 5th International Conference on Computational and Information Sciences (ICCIS, 2013), pp: 1537-1540.

William, S., 2005. Cryptography and Network Security: Principles and Practices. 4th Edn., Prentice Hall, Upper Saddle River, NJ.

Wu, C.F. and L.P. Huang, 2011. Developing the environment of information technology education using cloud computing infrastructure. Am. J. Appl. Sci., 8: 864-871.

Zehua, Z. and Z. Xuejie, 2009. Realization of open cloud computing federation based on mobile agent. Proceeding of the IEEE International Conference on Intelligent Computing and Intelligent Systems, 3: 642- 646.