A Hybrid Trust Computation Model for Cloud Services

Gure Sravani[1], CH.Kodanda Ramu[2]
M.Tech Scholar[1], Assistant Professor[2]
[1,2]Dept of CSE,Avanthi Institute of Engineering and Technology, Visakapatnam,A.P,India

Abstract: *Trust measurement is one of the interesting research issue in the field of trust management in cloud computing. The highly dynamic, distributed, and non-transparent nature of cloud services introduces several challenging issues such as privacy, security, and availability. Preserving consumers' privacy is not an easy task due to the sensitive information involved in the interactions between consumers and the trust management service. In this paper we propose an empirical model of trust management with various trust computation parameters and authentication and security can be maintained by elliptic curve digital signature algorithm. Our proposed model gives efficient results than traditional models.*

I. INTRODUCTION

The resources made available through cloud computing include hardwareand systems software on remote datacenter, as well as services basedupon these that are accessed through the Internet; these resources can bemanaged to dynamically scale up to match the load, using a pay-perresourcesbusiness model. Key features advertised are elasticity, multitenancy,maximal resource utilization and pay-per-use. These new features provide the means to leverage large infrastructures like data centresthrough virtualization or job management and resource management[1][2].

Cloud computing (or, more essentially, 'cloud') furnishes a market opportunity with a colossal potential both for proficiency and new business openings (particularly in benefit piece), and is practically sure to profoundly change our data innovation foundations[3], models and administrations. Not exclusively are there fetched reserve funds because of economies of scale on the specialist organization side and pay-as-you-go models, yet business hazard is diminished in light of the fact that there is less need to acquire cash for forthright interest in foundation. The appropriation of cloud computing may move rapidly contingent upon neighbourhood prerequisites, business setting and market specificities[4]. We are still in the beginning times however cloud advances are getting to be plainly received generally in all parts of the world. The monetary capability of cloud computing and its ability to quicken development are putting business and governments under expanded strain to receive cloud computing based arrangements.

Even though the buildup around cloud tends to urge individuals to imagine that itis an all-inclusive panacea, this is not the case and regularly promoters disregard the inborn complexities included by the cloud. There are various difficulties to giving cloud computing administrations[5] the need to follow nearby also, provincial controls, acquiring the important endorsements when information is gotten to from another purview, some extra intricacy in wording of administration, support and obligation characteristic to cloud, and an apparent absence of trust in cloud administrations. Numerous Chief Information Officers (CIOs) in vast undertakings distinguish security worries as the best explanation behind not grasping people in general cloud more forcefully, and not profiting from related cost improvements.

Cloud computing enables a new business model that supports ondemand, pay-for-use, and economies-of-scale IT services over the Internet. The Internet cloud works as a service factory built around virtualized data centres. Cloud platforms are dynamically built through virtualization with provisioned hardware, software, networks, and datasets. The idea is to migrate desktop computing to a serviceoriented platform using virtual server clusters at data centres. However, a lack of trust between cloud users and providers has hindered the universal acceptance of clouds as outsourced computing services. To promote multitenancy, we must design the cloud ecosystem to be secure, trustworthy, and dependable[6].

II. RELATED WORK

Trust is a social problem, not a purely technical issue. However, we believe that technology can enhance trust, justice, reputation, credibility, and assurance in Internet applications. To increase the adoption of Web and cloud services, cloud service providers (CSPs) must first establish trust and security to alleviate the worries of many users. A healthy cloud ecosystem should be free from abuses, violence, cheating, hacking, viruses, rumors, pornography, spam, and privacy and copyright violations. Both public and private clouds demand "trusted zones" for data, virtual machines (VMs), and user identity, as VMware and EMC 3 originally introduced[7].

Data integrity issues in the clouddiffer from those in traditional database systems. Cloud users are most concerned about whether data-center owners will abuse the system by randomly using private datasets or releasing sensitive data to a third party without authorization. Cloud security hinges on how to establish trust between these service providers and data owners. To address these issues, we propose a reputation-based trust-management scheme augmented with data coloring and software watermarking. Information about related trust models is available elsewhere[8][9].

The Cloud Security Alliance has recognized a hardly any basic issues for trusted cloud computing, also, a few late works examine general issues on cloud security and privacy.Public also, private clouds request diverse levels of security implementation. We can recognize among various administration level understandings (SLAs) by their variable level of shared duty between cloud suppliers and clients. Basic security issues incorporate information respectability, client privacy, furthermore, trust among suppliers, person clients, and client gatherings.

Cloud platforms are built on top of IaaS withsystem integration and virtualization middlewaresupport. Such platforms let users deployuser-built software applications onto the cloudinfrastructure using provider-supported programminglanguages and software tools (suchas Java, Python, or .NET). The user doesn'tmanage the underlying cloud infrastructure.Popular PaaS platforms include the Google AppEngine (GAE) or Microsoft Windows Azure.This level requires securing the provisionedVMs, enforcing security compliance, managingpotential risk, and establishing trust among allcloud users and providers[10].

Malware-based assaults, for example, worms, infections, what's more, DoS misuse framework vulnerabilities and give gatecrashers unapproved access to basic data. Unsafe cloud stages can cause organizations to lose billions of dollars and might upset open administrations. We propose a securityaware cloud engineering and distinguish the insurance instruments required.

Even though various models proposed by various authors from years of research, every model has its own advantages and disadvantages.In traditional model of trust computation, trust can be identified with static measures ,it may not give the optimal results and authentication is also an important factor while sharing the data between the nodes over cloud server.Static trust measures may not give optimal results while computing paths and Complex to implement practically and authentication and confidentiality are integrated parallelly

III. PROPOSED SYSTEM

We propose an empirical model of trust management between the nodes (here in this context it is between cloud service provider and consumer).We compute the cost matrix based on the trust matrics , which generates an optimal path. Authentication and data confidentiality can be maintained by Elliptic curve digital signature algorithm .sIn our work the system we proposed a strong curve theory for generating strong signature for the message. We implemented encoding algorithm which is based on the secret value using mathematical operations. Initially path request can be forwarded to the service process and compute the path interms of trust metrics like global trust, reputation metrics and mutual trust, every node can have average trust metric values, so service process optimal cost of the possible paths in terms of total trust cost and forwards the encoded cipher packets through the path.

- Trust metrics can be computed dynamically for computation of path
- Authentication and confidentiality are integrated parallelly
- Less time complexity

Cloud Service consumer itself is a node which receives the data packets from another node in trust management service layer, authentication should be done between the node in TMSL and requstedor subscribed node.

Route Cost Implementation:

Path between the requested node and destination node can be computed through so many intermediate nodes and intermediate servers. Service layer computes the path between the nodes based on the trust measures like global trust, reputation metrics and mutual trust, every node can have average trust metric values, so service process optimal cost of the possible paths in terms of total trust cost and forwards the encoded cipher packets through the path..

Route from source to destination can be computed with trust metrics like global trust, reputation metric and mutual trust, for every path cost can be computed by combing the all the metrics for respective node

Step1: Requested node selects the intermediate or destination node to transmit data packets

Step2: Request received by the processing module and generates the paths in topology

Step3: The Processing module computes the path with their global trust, reputation metric and mutual trust metrics

Step4: select optimal path (optimal communication cost) and transmits the data.

Cost= global trust + reputation metric + mutual trust

Secure key generation:

The generation of the public key in ECDSA involves computing the point, Q, where $Q = dP$. In order to crack the elliptic curve key, adversary Eve would have to discover the secret key d. Given that the order of the curve E is a prime number n, then computing d given dP and P would take roughly $2^{n/2}$ operations [1]. For example, if the key length n is 192 bits (the smallest key size that NIST recommends for curves defined over GF(p)), then Eve will be required to compute about 2^{96} operations. If Eve had a super computer and could perform one billion operations per second, it would take her around two and a half trillion years to find the secret key. This is the elliptic curve discrete logarithm problem behind ECDSA.

1. Select an elliptic curve E defined over a finite field F_p such that the number of points in $E(F_p)$ is divisible by a large prime n.
2. Select a base point, P, of order n such that $P \in E(F_p)$
3. Select a unique and unpredictable integer, d, in the interval [1, n-1]
4. Compute $Q = dP$
5. Sender A's private key is d
6. Sender A's public key is the combination (E, P, n, Q)

IV. CONCLUSION

We have been concluding our current research work with efficient path computation and authentication model through trust management technique. We use various trust measures to select the optimal nodes for computation of path . Once source and destination nodes are selected , authentication and key generation parameters exchanged and data can be encoded and decoded vice versa. Our proposed work gives more efficient results than traditional approaches.

REFERENCES

[1] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising From Cloud Computing," in *Proc. CloudCom'10*, 2010.

[2] E. Bertino, F. Paci, R. Ferrini, and N. Shang, "Privacy-preserving Digital Identity Management for Cloud Computing," *IEEE DataEng. Bull*, vol. 32, no. 1, pp. 21–27, 2009.

[3] E. Friedman, P. Resnick, and R. Sami, *Algorithmic Game Theory*. New York, USA: Cambridge University Press, 2007, ch. Manipulation-Resistant Reputation Systems, pp. 677–697.

[4] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.

[5] F. Skopik, D. Schall, and S. Dustdar, "Start Trusting Strangers? Bootstrapping and Prediction of Trust," in *Proc. of WISE'09*, 2009.

[6] H. Guo, J. Huai, Y. Li, and T. Deng, "KAF: Kalman Filter Based Adaptive Maintenance for Dependability of Composite Services," in *Proc. of CAiSE'08*, 2008.

[7] T. Dillon, C. Wu, and E. Chang, "Cloud Computing: Issues and Challenges," in *Proc. of AINA'10*, 2010.

[8] Y. Wei and M. B. Blake, "Service-oriented Computing and Cloud Computing: Challenges and Opportunities," *Internet Computing,IEEE*, vol. 14, no. 6, pp. 72–75, 2010.

[9] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," Sep 2011, accessed: 05/06/2012, Available

at: http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145 cloud-definition. pdf.

[10] O. David and C. Jaquet, "Trust and Identification in the Light of Virtual Persons," pp. 1–103, Jun 2009, accessed 10/3/2011.

BIOGRAPHIES

CH.Kodandaramu working as a Assistant Professor in Avanthi Institute of Engineering and Technology in Department of CSE. He completed M.Tech and pursuing P.hd. His interests are data mining, network security, and cloud computing.

GureSravani pursuing M.Tech in Avanthi Institute of Engineering and Technology in Department of CSE. Her interests are data mining, network security.