High Performance AAA Security for Cloud Computing in Hierarchical Model

Nisha Bawaria
Department of Computer Science Engineering
M.Tech (CSE), BITS, Bhopal

Kamlesh Namdeo
Department of Computer Science Engineering
M.Tech (CSE), BITS, Bhopal

Pankaj Richhariya
Department of Computer Science Engineering
M.Tech (CSE), BITS, Bhopal

ABSTRACT
In internet and text documents tons of vital information is available. This side-information is available in documents as beginning information, the links within the documents, user-access behavior from internet logs, or different non-textual characteristics which are embedded into the text document. This side information is employed in document clustering of such documents bunch. This information can embody noisy information as well; therefore it's tough to use it with efficiency. Thus correct algorithms are needed to use such information in document clustering to avoid noise from the extracted clusters. We'd like a properly dominated ways to perform the mining method to optimize the benefits got from mistreatment of this side information. In this work, we are improving the planning of AAA algorithm to accommodate high security and efficiency of the system.

Keywords
AAA Algorithm, Security, Cloud Computing, Hierarchical Model

1. INTRODUCTION
The Cloud computing provides the capability to storage the resources, used for multipurpose computing task on a metered basis. It is used for enabling convenient, as per the requirement network access model to a shared collection of configurable and reliable resources that are rapidly provisioned and released with minimal user management effort or service provider communication [1]. Cloud computing were developed from technologies and business approaches that emerged over a number of years.

The important elements in the origination of cloud computing are utility computing, Grid computing, Autonomic computing, Platform Virtualization, software as a service (SaaS), Service Oriented Architecture (SOA) etc. The security of cloud services and access control of the environment are essential components of an organization [2]. Various kinds of application and services are provided by the Cloud.

The upper layer is Software-as-a-Service (SaaS) which provides it users with able to use applications. SaaS is trusted service to access application functionality through a web browser. The lower layer is Infrastructure-as-a-Service (IaaS), provides basic infrastructure elements like storage, memory, CPU's and Servers. In the middle, Platform-as-a-Service (PaaS), allows deploying and dynamically scaling numerous applications like Google App Engine is an example for an PaaS. Either web browser or net service are used to access all these Cloud services SaaS and IaaS respectively and for Paas both approach we can used [3]. This paper describes an AAA-based security management framework for cloud applications, called Diameter AAA, based on Diameter base.

2. CLOUD COMPUTING SECURITY ISSUES
Rapidly growing organization is differentiating by their increasing business competition and changing ICT landscape. Today's market of cloud computing and their awareness are heavily weighted toward reliability and security concerns problems. When an organization gets into the cloud then its data could resides on the same machine as that of a competitor's. Mostly recent surveys shows that the security concerns are a major reason that's why only 2% are actually implementing cloud based services even more than 50 % of organizations have cloud-based services in their plans [6].

There are various major security threats to Cloud Computing which necessarily leads cloud users to rethink against cloud systems before move into the cloud [7]. They are: Abuse and Nefarious Use of Cloud Computing. Insecure Application Programming Interfaces:

- Malicious Insiders.
- Shared Technology Vulnerabilities.
- Data Loss/Leakage.
- Account, Service & Traffic Hijacking.
- Unknown Risk Profile.

Attacker continues to influence new technologies to develop their reach and improve the success of their activities. Cloud service providers are aggressively being targeted because their relatively weak service registration systems facilitate anonymity and service provider's fraud detection capabilities are limited.

Nowadays, Cloud computing is improving its security and most of the online survey regarding cloud computing conclude that the security concern is in the highest priority on the cloud domain. Online survey was carried out in order to find out the security problems in private cloud, public cloud and hybrid cloud from the service providers viewpoint (figure 3). The driving factors from the survey that motivate us to conduct research on the security domain of cloud computing.

3. THE DIAMETER-AAA COMPUTING MODEL FOR CLOUD COMPUTING
The "Diameter-AAA Application for Authentication, Authorization and Accounting in cloud Applications". The proposed areas of application for Diameter-AAA are such applications which we used as a Diameter server for authentication, authorization and accounting of their users. Also, a Diameter client with input data authenticates its user through the web browsers.

Moreover, it allows the Diameter client to authorize the access to applications or services offered by the cloud service provider. An important usage circumstance of Diameter AAA is deployment in security management frameworks where there may be different trust relationships between the cloud service provider, the authentication server and users. This means that the Diameter-AAA specially addresses the authentication, authorization and accounting requirements for the purpose of security management. Hence, only privileged users across their enterprise and access to the applications and services that they require, when they require them, and all unauthorized users are blocked. In Cloud environments, these controls are more critical because it supports a large enterprise and various communities of users. For authorized users to quick availability of cloud services use Diameter-AAA is required to simplify user authentication for both the cloud service provider and hosted applications. This three A's (AAA) is a core cost effective driver behind a Cloud Computing services and applications to charging the users according to their actual usage. The figure 4 shows that the model architecture of Diameter-AAA where various network elements like NAS, Router through which application flows need to pass, a cloud of AAA servers, and an authorizing entity.

There may be more than one network elements that needs to interact with the AAA cloud even though the figure only represents one for clarity. The end users authorization request sends via the AAA cloud (Diameter Application) to the diameter servers. AAA cloud entities will route the request to a designated Diameter-AAA server based on incoming specific services reservation request.

The role abdominal aortic aneurysm clouds (Diameter Application) are like agents and accountable for:

- It is often used for meditation of requests from variety of distributed NAS instrumentation and performs an action like relay, proxy, redirect, and translation agents.
- It will handle process to either requests or responses and conjointly accountable for load reconciliation between diameter servers.
- In cloud network, there'll be multiple diameters, therefore it will kind the requests supported services reservation request and forward towards the individual authentication server.

4. DIAMETER PROTOCOL

The Diameter protocol permits peers to exchange a spread of messages.

The base protocol provides the subsequent facilities:

- Delivery of AVPs (attribute price pairs)
- Capabilities negotiation, PRN in
- Error notification
- Extensibility, through addition of recent commands and AVPs

All knowledge delivered by the protocol is within the type of AN AVP. a number of these AVP values are utilized by the Diameter protocol itself, whereas others deliver knowledge related to specific applications that use Diameter. AVPs is also else at random to Diameter messages, goodbye because the needed AVPs are enclosed and AVPs that are expressly excluded don't seem to be enclosed. AVPs are utilized by base Diameter protocol to support the subsequent needed features:

- Transporting of user authentication data, for the needs of sanctioning the Diameter server to demonstrate the user.
- Transporting of service specific authorization data, between shopper and servers, permitting the peers to come to a decision whether or not a user's access request ought to be granted.
- Exchanging resource usage data, this can be used for accounting functions, capability coming up with, etc.
- Relaying, proxying and redirecting of Diameter messages through a server hierarchy.

The Diameter base protocol provides the minimum necessities required for AN abdominal aortic aneurysm transport protocol, PRN by NASREQ, Mobile IP, and ROAMOPS. the bottom protocol isn't supposed to be utilized by it, and should be used with a Diameter application, like Mobile information science [10]. The Diameter protocol was heavily galvanized and builds upon the tradition of the RADIUS [1] protocol.

Any node will initiate a call for participation. in this sense, Diameter may be a peer to look protocol. during this document, a Diameter shopper is AN access device that initiates a call for participation for authentication and/or Authorization of a given user. A Diameter agent may be a node that doesn't demonstrate and/or authorize messages domestically, like proxies and relay agents. A Diameter server is one that performs authentication and/or authorization of the user supported some profile. A Diameter node might act as AN agent sure enough requests whereas act as a server for others.

The Diameter protocol conjointly supports server initiated messages towards access devices, like a call for participation to abort service to a specific user.

5. LITERATURE REVIEW

The Cloud computing offers numerous services and internet based mostly applications over the net. With the tremendous growth within the development of cloud based mostly services, the protection issue is that the main challenge and today's concern for the cloud service suppliers. This paper describes the management of security problems supported Diameter abdominal aortic aneurysm mechanisms for authentication, authorization and accounting (AAA) demanded by cloud service suppliers. This paper focuses on the mixing of Diameter abdominal aortic aneurysm into cloud system design. [1]

Cloud computing offers AN exceptional physical property of resources and memorable economic benefits within the data Technology sector. It conjointly provides AN infrastructure for process massive and complicated scientific knowledge for data processing applications. Whereas giving compelling outturn gains, it conjointly introduces many challenges associated with security, economical storage of knowledge, and performance. We have a tendency to initial gift the fundamentals and a short history of cloud computing; followed by its edges, design, implementation and applications. Finally, we offer AN insight into the problems and challenges related to cloud computing. [2]

Cloud computing is an online based mostly model that modify convenient, on demand and pay per use access to a pool of

shared resources. it's a replacement technology that satisfies a user's demand for computing resources like networks, storage, servers, services and applications, knowledge security is one in every of the leading considerations and first challenges for cloud computing. This issue is obtaining additional serious with the event of cloud computing. From the consumers' perspective, cloud computing security considerations, particularly knowledge security and privacy protection problems, stay the first matter for adoption of cloud computing services. This paper analyses the essential drawback of cloud computing and describes the info security and privacy protection problems in cloud. [3]

Security challenges are still among the most important obstacles once considering the adoption of cloud services. This triggered lots of analysis activities, leading to an amount of proposals targeting the varied cloud security threats. Aboard with these security problems, the cloud paradigm comes with a replacement set of distinctive options, that open the trail toward novel security approaches, techniques, and architectures. This paper provides a survey on the realizable security deserves by creating use of multiple distinct clouds at the same time. Numerous distinct architectures are introduced and mentioned in keeping with their security and privacy capabilities and prospects. [4]

Cloud computing brings during a ton of benefits for enterprise IT infrastructure; virtualization technology, that is that the backbone of cloud, provides simple consolidation of resources, reduction of value, area and management efforts. However, security of vital and personal knowledge may be a major concern that still keeps back lots of shoppers from switch over from their ancient in-house IT infrastructure to a cloud service. Existence of techniques to physically find a virtual machine within the cloud, proliferation of computer code vulnerability exploits and cross-channel attacks middle virtual machines, all of those along will increase the danger of business knowledge leaks and privacy losses.

This work proposes a framework to mitigate such risks and engineer client trust towards enterprise cloud computing. Everyday new vulnerabilities are being discovered even in well-engineered computer code product and also the hacking techniques are becoming subtle over time. During this state of affairs, absolute guarantee of security in enterprise wide science system looks an overseas possibility; computer code systems within the cloud are at risk of security attacks. Sensible answer for the protection issues lies in well-engineered attack mitigation arrange. At the positive facet, cloud computing features a collective infrastructure which may be effectively accustomed mitigate the attacks if AN acceptable defense framework is in situ. We have a tendency to propose such AN attack mitigation framework for the cloud. Computer code vulnerabilities within the cloud have totally completely different severities and different impacts on the protection parameters (confidentiality, integrity, and availability).

By exploitation Andre Markoff model, we have a tendency to unendingly monitor and quantify the danger of compromise in numerous security parameters (e.g.: amendment within the potential to compromise the info confidentiality). Whenever, there's a major amendment in risk, our framework would facilitate the tenants to calculate the time unit to Security Failure (MTTSF) cloud and permit - hem to adopt a dynamic mitigation arrange. This framework is AN add-on security layer within the cloud resource manager and it may improve the client trust on enterprise cloud solutions. [5]

6. PROBLEM STATEMENT

The diameter-based accounting model for cloud environment is divided in to two:

Prepaid accounting system and

Postpaid accounting systems.

In both the cases, the accounting server sends the Internet Protocol Detail Record (IPDR) packet computed previously to AAA server. So the transaction is decreased the credit with the coordination of the accounting server and AAA server. Based on accounting policy, the cloud user usage table must be updated accordingly depend on usage of service or resources in the cloud. We can enhanced the proposed work as Future work which will include additional authentication methods for mobile cloud and a full performance evaluation based on given model implementation.

Processing time in whole cloud for AAA security is much higher and will cause severe performance degradation.

7. PROPOSED WORK

From the problem identified we have proposing to enhance the performance of the existing work by applying a hierarchical mechanism for solving the problem. The work shall be implemented in following steps:

A private/public cloud shall be implemented using C# where a web application shall be executed multiply to map the cloud

User will register on web application

A Diameter server and client mapping application shall be developed and made available on each web application

Users will add web resource for their own use.

User authentication and authorization shall be done whenever user starts using allocated resources.

Accountability is maintained for the user in the cluster server to which user belongs to.

Each cluster server shall communicate with a centralized server to maintain the accounting of the users whenever a user stops using the service.

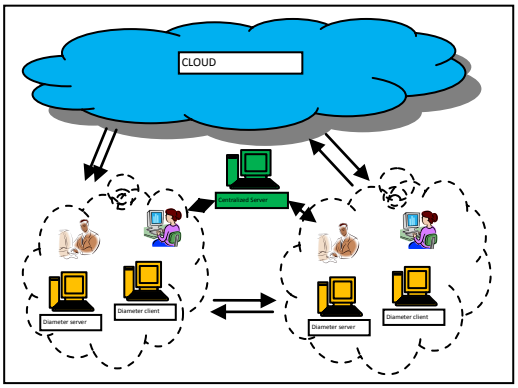

Figure 1: Architecture of the Proposed Work

8. CONCLUSION

With the emergence of cloud computing as a paradigm, presented approach for access control and identity management for cloud environment somehow fulfill the today's security challenges and provide trustful environment for consumers as well as service provider. The suggested framework that has been developed with the same

requirements that bridge the gap between application authentications in distributed network. Authentications and service authentication by effectively bringing network-based access control model to the service layer. Diameter-AAA provides authentication, authorization and billing services and is also able to handle identity attributes based on mUltiple different domains. We can used it as global authentication server which can be implement as central and secure authentication system that handles multi cloud environment as well as single cloud service provider. The similar draft is also partially available as an internet draft [14].

9. REFERENCES

[1] Sah, S.K.; Shakya, S.; Dhungana, H., "A security management for Cloud based applications and services with Diameter-AAA," Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on , vol., no., pp.6,11, 7-8 Feb. 2014 doi: 10.1109/ICICICT.2014.6781243

[2] Sinha, N.; Khreisat, L., "Cloud computing security, data, and performance issues," Wireless and Optical Communication Conference (WOCC), 2014 23rd , vol., no., pp.1,6, 9-10 May 2014 doi: 10.1109/WOCC.2014.6839924

[3] Dinadayalan, P.; Jegadeeswari, S.; Gnanambigai, D., "Data Security Issues in Cloud Environment and Solutions," Computing and Communication Technologies (WCCCT), 2014 World Congress on , vol., no., pp.88,91, Feb. 27 2014-March 1 2014 doi: 10.1109/WCCCT.2014.63

[4] Bohli, J.-M.; Gruschka, N.; Jensen, M.; Iacono, L.L.; Marnau, N., "Security and Privacy-Enhancing Multicloud Architectures," Dependable and Secure Computing, IEEE Transactions on , vol.10, no.4, pp.212,224, July-Aug. 2013 doi: 10.1109/TDSC.2013.6

[5] Datta, E.; Goyal, N., "Security attack mitigation framework for the cloud," Reliability and Maintainability Symposium (RAMS), 2014 Annual , vol., no., pp.1,6, 27-30 Jan. 2014 doi: 10.1109/RAMS.2014.6798457

[6] Peter Mell and Tim Grance, "Effectively and Securely Using the Cloud Computing Paradigm",National Institute of Standards and Technology (NIST) Information Technology Laboratory, October, 2009.

[7] P. B. Maxine Singer, Genes & Genomes: a Changing Per-spective. University Science Books, Mill Valley, CA, 1991.

[8] Raj Kumar Buyya, James Broberg and Andrzej Goscinski, "Cloud Computing Principles and Paradigms", A JOHN WILEY & SONS, INC., PUBLICATION 2011.

[9] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, "Diameter Base Protocol," RFC 3588 (Proposed Standard), Sep. 2003.

[10] D. Sun, P. McCann, H. Tschofenig, T. Tsou, "Diameter Quality-ofService Application" , Internet Engineering Task Force (IETF), May 2010.

[11] Balachandra Reddy Kandukuri , Ramakrishna Paturi V, Dr. Atanu, "Cloud Security Issues", 2009 IEEE International Conference on Services Computing.

[12] Security Guidance for Critical Areas of Focus in Cloud Computing, release on March 20 I O. DOl http://www.cloudsecurityalliance.org/topthreats/csathreats.v I .0. pdf

[13] H. Hakala, L. Mattila, J.-P. Koskinen, M. Stura, and J. Loughney, "Diameter Credit-Control Application," RFC 4006 (Proposed Standard), Aug. 2005.

[14] P. Jaeger, et aI., "Cloud Computing and Information Policy: Computing in a Policy Cloud?" Journal ofinformation Technology & Politics, vol. 5(3), pp. 269-283, 2008.

[15] H. Lim, et aI., "Automated Control in Cloud Computing: Challenges and Opportunities," in Proceedings of the First workshop on Automate Control for Datacenters and Clouds (ACDC '09), 2009, pp. 13-18.

[16] L. Youseff, M. Butrico, and D. Da Silva, "Toward a unified ontology of cloud computing," in Grid Computing Environ-ments Workshop, GCE'08, 2008.

[17] C. Weinhardt, A. Anandasivam, B. Blau, N. Borissov, and et aI., "Cloud computing a classification, business models, and research directions," vol. I, no. 5, pp. 391-399, 2009