Study on Secure Cloud Computing with Elliptic Curve Cryptography

Gopinath V [1], Bhuvaneswaran R.S[2]

[1] Sathyabama University, Department of Science and Humanities, Chennai, India

[2] Anna University, Department of Computer Science & Engineering, Chennai, India

Abstract

Cloud computing plays a major role by providing different resources in the form of web services like tax calculation web service, stock information web service, e-banking web service etc. But we can rely on cloud computing only when these web services are really secure enough to use. In this paper, a design of a security system for Cloud Computing is proposed using Elliptic Curve Cryptography (ECC) to secure XML web service and associated application. To further add on, a digital ECC key is being utilized by the XML Web Services security component. It secures the data transmission over the entire network route from the client to the remote server, and effectively improves the data processing speed of the server. The design is experimented with customized java coding and its performance is analyzed and compared with existing scheme. The design is found to be more secure and faster based on the preliminary results.

Keywords: *Cloud Computing, XML, Web Services security, Elliptic Curve Cryptography, private cloud.*

1. Introduction

Cloud has given a new approach to make IT a real utility which is global and complete for the end users by providing computational web services. Web services are programmable and reusable. They are available anywhere via the internet. Programs built using this model will run across multiple websites extracting information from each of them and combining and delivering it in a customized form to any device anywhere in the world. The potential of web service is unlimited. For example, a software company may provide a web service to calculate income tax. Any company that wants to calculate income tax can subscribe to this web service. The company offering this web service can dynamically update it to accommodate new taxation rates. The subscribers need not to do anything to get the new

updates. In future a collection of such web services may replace packaged software. It is often observed that whenever the user works with user interface in order to access these web services, users sensitive data including login and password etc. are being extracted by capturing the keystroke on the keyboard with the use of software such as Spyware, Trojans etc. Whenever we use a web service of cloud computing in such infected computers there is a danger of our sensitive data being hacked in spite of all the precautionary measures uploaded on our computers.

In this paper, we have proposed a secure use of cloud computing frame work based on Web Services Security gateways is aimed at providing a high level design of the SSL VPN. The proposed security concept improves the level of protection that the VPN currently supports by connecting the peer to peer network through an Elliptic Curve Cryptography and facilitates the realization of Peer to Peer Network to interact with web services of cloud computing.

When cloud offers a high level of confidentiality, safety and privacy to user's sensitive data, the usage of web services provided by cloud computing will be more. SSL VPN, ECC will play a major role in providing those security features to web services.

The XML-based interoperable characteristics create a lot of challenges when it comes for implementing security for Web service over the internet, especially in Cloud network. To meet the requirements of Web Services security, Many efforts have recently been made [2], [3] are noteworthy.

The rest of this paper is organized as follows. Section 2 discusses about the related works. Section 3 is the proposed framework of Integrated Security Solution for private cloud. Section 4 gives the details of analysis and experimental results. Section 5 is the conclusion with the future work.

2. Related Works

In [1], VPN framework which is suitable for the application of cloud computing is based on hub-and-spoke and bipartite. The user has to connect to hub-GW by using VPN. The Management of hub-GW uses bipartite, which divides users into categories of enterprise and cloud computing provider, with only intercategory users allowed connecting each other. VPN frameworks can be divided largely in full-mesh and hub-and-spoke. In full-mesh, every node is connected directly to others by dedicated lines. It can make sure rate quality and performance, in hub-and-spoke, there's one node called hub-gateway (Hub-GW), and rest nodes are spoke nodes. Hub-GW is charged with the connection to all spoke nodes. In [2], web service and traditional network based application utilize the same digital ECC key, SOAP message security, ECC algorithm and other supporting functions. This security scheme addresses authentication, authorization, confidentiality, integrity and non-repudiation issues. In [2], ECC cryptography is helps to increase the speed of encryption and decryption and shortening the CPU execution cycle. The algorithm points in [3] relies on a mathematical problem that is more difficult for hackers to attack than the current encryption; it can offer equivalent security with substantially smaller key sizes.

Aforementioned algorithm tends to have some limitations. Web service security system is not available in the framework. Security is provided only when the connection is established and RSA algorithm is inbuilt in SSL.Here the SSL uses RSA 128- bit security key, the effective cost of public key operations is determined by the frequency of session reuse, which eliminates the need for public-key operations for some transactions, the cost of encryption and hashing depends on the amount of data transferred.
In this paper, XML web service security and secured framework component with ECC is proposed.

3. Design of security system for Private Cloud VPN with ECC

To The proposed system is aimed at providing a high level design of the SSLVPN with ECC, which is applied on a Private Cloud. It helps in connecting the peer to peer network through an Elliptic Curve Cryptography. The proposed security concept improves the level of protection that currently supports the Private Cloud VPN and facilitates the realization of Peer to Peer Network. Figure. 3.1 shows about the high level design of the system.

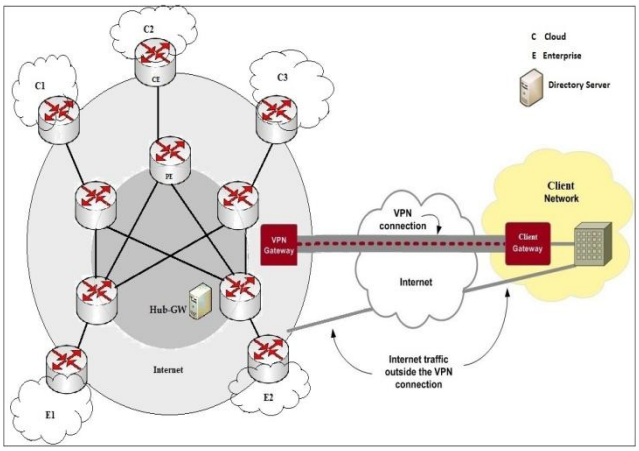


Fig. 1 High level design of the Private Cloud VPN system.

3.1 Private Cloud in VPN

Private Cloud VPN frameworks can be divided largely into full-mesh and hub-and-spoke. In full mesh every node is connected directly to others by dedicated lines. In hub-and-spoke, there is one node called hub-gateway (Hub-GW), and the rest nodes are spoke nodes. Cloud VPN framework incorporate the concept of bipartite network [1]. There are three roles in this framework: CE, PE and directory server. CE is charged with routing at spoke end, PE is charged with routing and forwarding at hub-GW.Directory server is authentication server. If the enterprise needs to connect with other cloud services, it only takes to activate the corresponded routes at directory server.

3.2 ECC Encryption in VPN

ECC encryption technology addressed the weakness of RSA encryption in public key structure as it helps to increase the speed of encryption and decryption and shortening the CPU execution cycle as well as helps in improving the data processing speed of the server [4]. The modified ECC is more secure and difficult for hackers to attack than the current encryption; it can offer equivalent security with substantially smaller key sizes [14].

3.3 WebServices Security and framework component

VPN Server Web service application is used by the client. The client dynamically loads the XML Web services security component to provide integrated security solution. It secures both web services and traditional network based application. Both utilize the same digital ECC key, SOAP message security, ECC algorithm and other supporting functions [2]. The XML web services with ECC component is added to the existing VPN to provide integrated security solution for securing both

XML web service and traditional network applications, it uses the same digital ECC key that is used by the VPN Server. Both VPN and web services share the same key, as well as same access control mechanism. Web service security unit strictly applies more measures if the requests are from outside the VPN; whereas requests from the VPN require no such measures. This component has been built with Microsoft (MS) packages of XML security, SOAP security, and ECC algorithm, other supporting function based on MS Framework 4.0

3.4 Dataflow in the integrated system

VPN contains SSL and ECC; VPN client receives the network traffic from network tap (TAP) adapter [16]; After receiving the network traffic, application traffic is redirected to TAP adapter, it searches whether the traffic needs to be sent through tunnel, if network traffic needs to be tunneled then the VPN client applies the encryption algorithm to the network traffic. Finally it sends the encrypted network traffic to VPN server via the physical adapter. When the thumb drive is connected, connection is done automatically without the requirement for any pre-installed software and it enables the secured generation of public key and encryption and decryption. That is, we establish the secure data transmission when the portable device is connected, otherwise gets disconnected automatically.

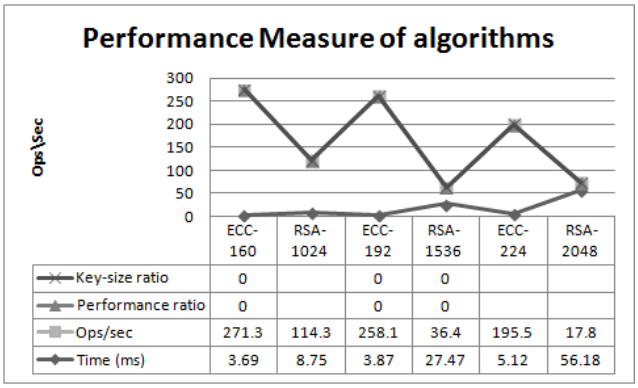
4. Analysis Result

Cloud computing is characterized by the accessibility at any time as needed, with purpose of reducing managerial costs and increasing efficiency in operation with Secured way. The ECC VPN that connects cloud computing should possess the above mentioned characteristics. The network environment should be easy to establish, update or erase connections according to the demand for cloud computing, so as to mitigate the complexity of network management. Given such presupposition, the application of ECC VPN in cloud computing should satisfy the below requirements.

Table 1: Comparison between Existing framework and proposed framework

Analysis Report	Existing frameworks	Proposed framework
Configuration Management	Single	Single
Fault Management	Simple	Simple
Performance Management	Integrated	Integrated
Security Management	Support directory server	support encrypted data and directory server
Accounting Management	Convenient	Convenient
Confidentiality	File encryption not provided	Symmetric key
Authentication	Not provide	Password-based
Access Control	Exposure to the normal area	Encryption of security area information
Impersonation Attack	No impersonation	Two stages of user authentication
Efficiency	Easy to implement	Easy to implement

Private cloud VPN replacing RSA with ECC in the SSL protocol. ECC is a public key cryptography technique providing 160- bit Security key, the effective cost of public key operations is determined by the frequency of session reuse which eliminates the need for public-key operations for some transactions, the cost of encryption and hashing depends on the amount of data transferred. We used the OpenSSL speed program to measure RSA decryption and ECDH operation for different key sizes. Results for the proposed system, shown in Figure 4.1 Performance Measure of algorithms



The proposed security scheme is employed as an add-on feature to the Private Cloud standard. It accommodate a wide range of configurations, including remote access, site-to-site VPNs, Wi-Fi security, and enterprise size solutions provide many options for controlling the security of the VPN client and options for protecting the security of the server itself

5. Conclusions

The above analysis suggests that the framework is suitable for the application of cloud computing as it is based on hub-and-spoke and bipartite. The user has to connect hub-GW by using VPN which is bounded with ECC to accept the performance benefits of SSL clients, especially for the

servers as the security needs are arising. The proposed security scheme improves the Level of protection in existing private cloud. It secures data transmission over the entire network route by utilizing the default P2P network over the private cloud, The potential incompatibilities that arise from the simultaneous use of ECC, as well as the impact of user mobility on VPN operation is considered, and detailed solutions are proposed, Also, we have focused on security aspect of web services and Integration of the Web Services security component with the Application server is proved to be feasible and efficient.

References

[1] Wen-Hwa Liao, Shuo-Chun Su "A Dynamic VPN Architecture for Private Cloud Computing "Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on Digital Object Identifier: 10.1109/UCC.2011.68, 2011, PP 409 – 414.

[2] A. Goldberg, R. Buff, A. Schmitt, "Secure Web Server Performance Dramatically Improved by Caching SSL Session Keys", In Proc. of Workshop on Internet Server Performance, SIGMETRICS'98, Jun. 1998 pp 1-4.

[3] Wen Shi Chen , Chunxiao Liu "The Applied Research of ECC Encryption Algorithm in VPN Technology " Inter-net Technology and Applications (iTAP), 2011 ,PP 1 – 4

[4] Ying Liu, Yeap, T.H."Securing XML Web Services with Elliptic Curve Cryptography ", Electrical and Computer Engineering, 2007. CCECE 2007,PP 974 – 977

[5] C. Nuangjamnong, S. P. Maj, and D. Veal, The OSI network management model capacity and performance management, the 4th IEEE International Conference on Management of Innovation and Technology (ICMIT), 2008

[6] Enomoto. N, Yoshimi, Hideo, Sai, C,"A secure and easy remote access technology",Information and Telecommunication Technologies, 2005. APSITT 2005 Proceedings. 6thAsia-Pacific Symposium on Digital Object Identifier: 10.1109/APSITT.2005.203686 PP:364 – 368

[7] N. Koblitz, "Elliptic curve cryptosystems", Mathematics of Computation, 48:203-209, 1987.9. Fernandes, F.R.,Machado, R.J.S.,Ferreira, J.M. ,Gericota, M.G. "Gatewaying IEEE 1149.1 and IEEE 1149.7 test access ports "On-Line Testing Symposium (IOLTS), 2012 IEEE 18th International ,June 2012,PP 136 - 137.

[8] S.Adreozzi, P. Ciancarini, D. Montesi, R. Moretti, "To-wards a model for quality of web and grid service" In Proc 13th IEEE international Workshops on Enabling Technologies: Infrastructure for Colloborative Enterprises (WET ICE'04), 2004, page 271-276.

[9] D. Gouscos, M. Kalikakis, and P. Georgiadis. "An approach to modeling Web service QoS and provision price", in Proceeding 3rd International Conference on Web Information Systems Engineering Workshops, pages 121-130, 2003.

[10] J.P Thomas, M.Thomas and G.Ghinea "Modeling of Web service flow", in Proceeding IEEE International Conference on E-Commerce (CEC 03), pages 391-398, 2003.

[11] V. Cardellini, E. Casalicchio, M. Colajanni, "A performance study of distributed architectures for the quality of Web services", in Proceeding 34th Annual HawaiiInternational Conference on System Sciences,2001.

[12] NIST, The NIST Definition of Cloud Computing (Draft), http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf, Jan. 2011

[14] Cloud Security Alliance, top threats to cloud computing, https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, Mar. 2010

[15] J.D. Meier, Principal PM, Paul Enfield, Windows Azure Security Notes, http//go.microsoft.com/?linkid=9741707, Mar. 2011

[16] Michael Armbrust et al., A View of Cloud Computing, Communications of the ACM, Association for Computing Machinery, Vol. 53, No. 4, pp.50-58, Apr. 2010

[17]Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1,