Intermediatery Proxies By Scalable and Robust Network Content Processing

[1]Satya P Kumar Somayajula, [2]Sesi Kala Bapatla
Dept. of CSE, Avanthi Insitute of Engg. & Tech, Tamaram, Visakhapatnam, A.P., India.

Abstract
In today's world, more and more business transactions are moving to the Web, including business and consumer e-commerce, financial services, and other transactions requiring the transmission of personal or confidential information. Ensuring the security of these transactions and the data they contain is of the utmost importance.. Protection and secure exchange of web documents is becoming a crucial need for many Internet-based applications. Securing web documents entail addressing two main issues confidentiality and integrity. Ensuring document confidentiality means that document contents can only be disclosed to authorized security policies, whereas by document integrity we mean that the document contents are correct with respect to given application domain and that the document contents are modified only by authorized policies. In this paper, we propose an approach that addresses data integrity and confidentiality in content adaptation and caching by intermediaries. Our approach permits multiple intermediaries to simultaneously perform content services on different portions of the data. Our protocol supports decentralized proxy and key management and flexible delegation of services.

Keywords
Data Sharing; Distributed System; Confidentiality; integrity; security; ECC.

I. Introduction

While the requested contents are not cached or out of date is the contents transfer from the content server to the clients. If there is a cache hit, the network bandwidth utilization can be reduced. A cache hit also reduces access latency for the clients. System performance thus improves, particularly when a large amount of data is complicated. Besides this improvement, caching makes the system strong by letting caching proxies provide content distribution services when the server is not available. With the appearance of various network appliance and assorted client environments, there are other relevant new requirements for content services by intermediaries. For example, content may be altered to satisfy the requirements of a client's security policy, device capabilities, preferences, and so forth. Distributed cooperative application domains such as collaborative e-commerce distance learning, telemedicine, and e-government. Confidentiality means that data can only be access under the truthful authorizations. honesty means that data can only be made to order by endorsed subjects. The approach developed for securely transferring data from a server to clients are not suitable when data is to be transformed by Intermediaries. When a proxy mediates data transmission, if the data is enciphered during transmission, security is ensured. Much previous work has been done on data adaptation and content deliverance. It combines peer-to-peer systems and Web-based content deliverance. In such a model, integrity is imposed by using metadata express modification policies particular by content owner.

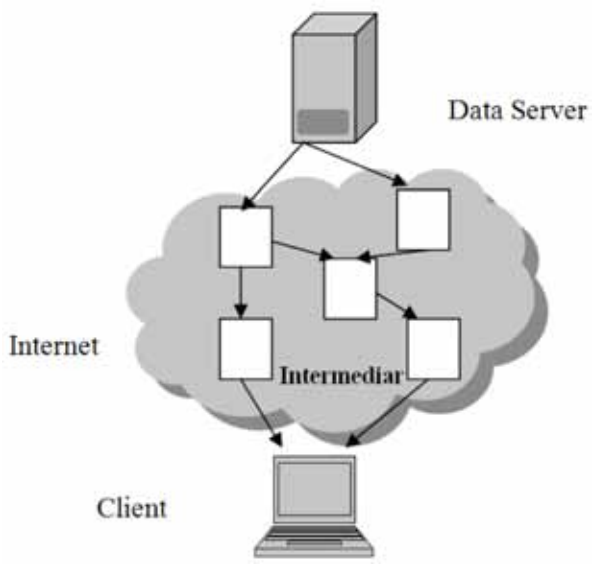

Fig. 1 : System Architecture

II. Preliminaries

A. Privileges and Functions Ofcontent Service

Every content service belongs to a service function. To interpret from a content service to a service function is a many-to-one method. Let us take an example a content service may compress the images with some less For example, a content service may compress images with less accuracy in order to decrease their size, or a content service may perform media translation such as from text to audio or a design alter such as from PDF to HTML. All these services belong to a transcoding purpose that changes the data from one format into another. To recap the basic content service functions that mediators can perform in Figure which is an extension of what we include some important classes of functions that are related to safety measures services, such as the function of virus scan.

Table 1 : Functions and corresponding privileges.

Function	Purpose/Description	privilege
Filter	Remove information	update
Annotate	Add information	update
Virus scan	Scan virus	Read,update
Transcode	Change to different format	update
Cache	Store for later use	Read
Watermark	Add watermarking	Update
Customize	Tailor for particular users	

In order to provide data security, an intermediary must have certain access privileges in order to enhance or ensure. Let us take an example if any proxy needs to transcode the data from text to audio, then it needs to have some privileges from the data server

that authenticates this proxy to perform this transaction function. A service function needs to update the requested data or not that tells based upon service function. There are two types of privileges that allow to identity that allow intermediaries to perform content service functions those are read function and update function. The read method allows a proxy to reserve and read the data. The update privilege allows a proxy to modify the data and read the data. The read privilege allows a proxy to read and reserve the data. The bring up to date privilege allows a proxy to read and modify the data. let us take an example that a proxy needs to have this privilege to execute a content filtering function.

<segment hash = encrypt value
Delegate key = pubkey1 delegate Hash = encryptvaue2>
<segi d> seg11 </seg id>
This is the virus scan result.

<seg id> seg18 </seg id>
This is the data for virus scan.

Fig. 2 : Example of data segments

B. Data Representation

We transmit our approach in the structure of XML because of its extensive use in Web services. XML can be used to supervise data, documents, graphics, and even multimedia data. It categorizes data into tag essentials. We describe an atomic element (AE) as either an attribute or an element including its starting and ending tags. A data segment is a set of elements to which the same access control guidelines apply. That is, if a proxy has a study (or write) advantage over a segment, the proxy has a study (or write) privilege over all the elements in the segment. We implement confidentiality by allow a proxy to contact only the segments that are acceptable by access control policy.

To implement authenticity and integrity, we rely on typical cryptographic primitives such as Elliptic-Curve Cryptography. The huge majority of the crop and principles that use public key cryptography for encryption and data digital signatures use RSA. The bit length for secure RSA use has greater than before over recent years, and this has put a heavier processing load o applications using RSA This burden has ramifications, especially for electronic commerce sites that conduct large numbers of secure transactions. Newly, a challenging system has begun to test RSA elliptic-curve cryptography (ECC). Already, ECC is showing up in consistency efforts.

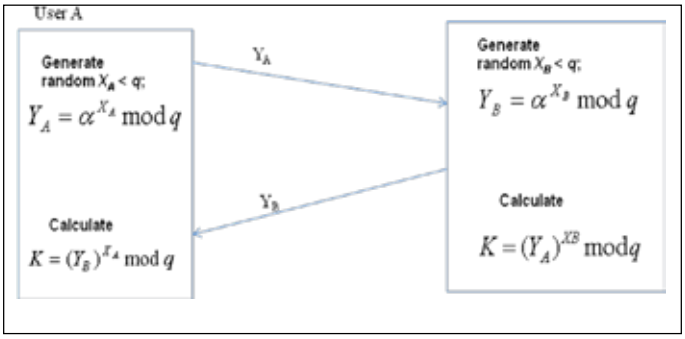

Fig. 3 : Diffie-Hellman calculation

The primary appeal of ECC compare to RSA is that it appears to offer equal security for a far smaller bit size, there by dipping processing operating cost. The figure shows a simple protocol that makes use of the Diffie-Hellman calculation. Assume that user A wishes to set up a connection with user B and use a secret key to encrypt messages on that connection. User a can generate a one-time private key XA, calculating YB, and sending YB to user A. Both users can now calculate the key. The necessary public values q and α would need to be known ahead of time. Otherwise, user A could pick values for q and α and include those in the first message. Public keys for digitally signing the data. Each segment has an encrypted hash value a associated with it. If a proxy has an modernize privilege over a segment, when the proxy complete update the segment, it produce a hash value by apply to the segment text, which also include the segment identifier, a one-way hash function and then encrypts the value with its private key.

C. Data Provider (DP) and P-Proxy

1. A DP is any entity that can offer the data request by a client. Thus, a DP may be either a data server or a cache proxy caching the data request by clients. In order to grant content services to clients, a DP has a collection of cooperative intermediaries that can achieve different content services.
2. Each DP maintains the in sequence about the services provided by each cooperative proxy in an intermediary profile table. The intermediary profile table supplies the public keys and the authorizations of proxies. Figure show an example of such a table. Because a proxy may provide numerous content services, it may appear in more than a a small number of different P-proxies maintain by a DP.
3. In Figure, proxy1 appears in both P-proxy1 and P-proxy4. Even though a P-proxy may group numerous proxies, only one proxy in such group perform the content service connected with the P-proxy on each request data.
4. For illustration, suppose that proxy1 is a virus scan proxy in P- proxy1 and that P-proxy1 also include proxy2. If proxy1 is congested, it can delegate to proxy2 the execution of the service. We refer to the proxy that is initially assigned to execute the operation on the data as the primary proxy (prim) of this P-proxy for the requested data.
5. In the earlier illustration, yet though proxy2 execute the virus scan, the primary proxy is proxy1.When a primary proxy p delegates the implementation of the content services to another proxy q, where p and q feel right to the same P-proxy, attributes delegate Key and delegate H ash are required, where delegate Key is q's public key, and delegate as h is the digital signature of q sign with its private key on the summary of process content. Note that q's public key is approved by p in p's signature.

Table 2 : Intermediary profile table

P-proxy name	Content servive	Proxy/Public key
P-proxy 1	Virus scan	Proxy1/pubk1, proxy2/pubk2
P-proxy 2	Logo-adding	Proxy3/pubk3
P-proxy 3	Ausio to text conversion	Proxy4/pubk4, proxy5/pubk5
P-proxy 4	Content filter	Proxy1/pubk1

D. Access Control System

Each DP has it's be the owner of security policy related to its data. The access control system of each DP enforces which proxies and clients can access which data. The inputs to the access control system include a client's request, the security policy and the intermediary profile table by the DP, and the data store. The access control system can return three possible access decisions:

1. **Deny:** This indicates that the DP does not have the data requested by the client, the client is not permissible to reception the data according to the DP's strategy, or no intermediaries in the DP's intermediary profile table exist or are allowed to change the data into the adaptation ask for by the client.
2. **Empty path:** This indicates that the client's applying for can be fulfilled without any intermediary's contribution.
3. **ACIS Path:** This specify that the client's relate for can be satisfied with the association of the Proxies planned in the return path. ACIS indicate access control in sequence structure, which specifies the privileges over the data for each P- proxy in the path

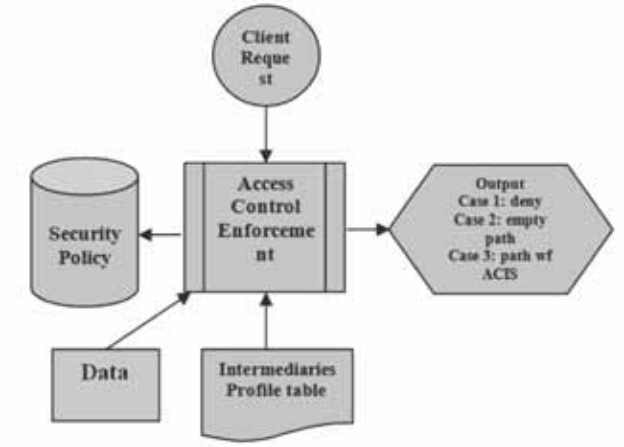

Fig. 4 : Access control system

We now grant details relating to paths and ACIS.

Let the next proxy to resolve whether the translation is done sincerely or some individual text has been welcoming. The necessities for the content service path are that the path should follow the same segment update-update order and update-read order. Namely, if a segment is updated by content services i and j, the order of i and j is important. For example, in the previous illustration , if segment seg is updated by both logo adding and audio-to-text conversion, then only after audio-to-text conversion can the logo be added to the segment. Thus, the content service production with text conversion must be placed before logo adding. Also, as the virus scan needs to read this segment, the virus scan must be placed after the logo-adding service.

The control information CIi for P-proxyi in a path also contains the corresponding incoming package templates and outgoing package templates. Each incoming package template has a predecessor associated with it. If a receiver receives from the same sender several packages at different times, the pid will help the receiver to determine which packages are referred to in its control information received from the DP. Each member can use its control information for integrity checking and secure communications.

III. Parallel Secure Content Protocols

In Parallel secure content service give the security assumptions are:

- Every DP has a group of P-Proxies that are cooperative with the DP.
- Every Proxy in a P-proxy is equal.
- Every P- proxies that can perform the content services requested by a client are operative.
- To access data without permission, thus violating data confidentiality or it may attempt to modify data without permission, thus violating.

A. Parallel Secure Content Service Data Protocol

1. Data Server Protocol

The algorithm is organized according to the following main phases:

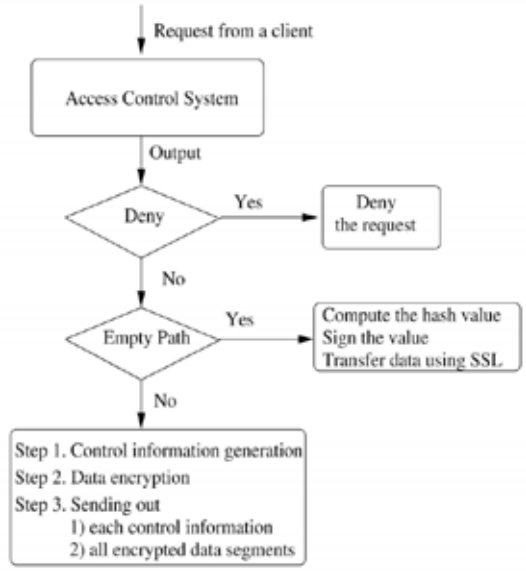

Fig. 5: Data server protocol for handling content service requests

(i). Initialization: First, for each participating P-proxy, the data server randomly orders the proxies in each P-proxy. The first one in the list is the primary proxy for this P-proxy. This random ordering avoids making certain proxies overloaded, especially when a proxy is being used in many P-proxies in a data server or a proxy appears in many DPs' intermediary profile table. This step also initializes each P- proxy's predecessors < Pred>, successors <succ> and segments <seg> that this P-proxy is authorized to access. For each P-proxy in Path, this step labels each segment that this P-proxy is authorized to access with a list of public keys of the P-proxy that can modify this segment. The list of keys starts with the primary proxy of the P-proxy, followed by other proxies' public keys in the P-proxy.

(ii). Generating the data Server's CI: The data server needs to send segments to corresponding P-proxies or to the client. Each P=Proxy must receive the segments that are allowed to access and send some or all of these segments to subsequent P-proxies ro the client. For each segment, the data server scans the P-proxies according to the content service. The data server repeats this activity until the first P-proxy that needs to update this segment. After the P-proxy updates the segment, it sends out the segment to the rest of the P-proxies or the client if they need to access it.

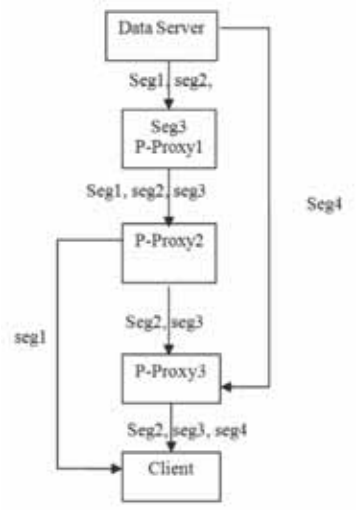

Fig. 9 : An example of control information

Once the data server has generate the control information and encrypted the data segments, it distributes them to the corresponding primary proxies and the client. The data server also provides a one-way hash function for the participating proxies and the client to verify the authentication of the data they received and to calculate a digest value for each segment they have updated.

(iii). Key Management : Here we have provided Public keys for signing and symmetric keys for encrypting contents. Even though the number of keys are used may be large, key management is quite simple, and there is a need for public key infrastructure. The Data Provider maintains intermediary profile table for storing public keys of proxies. Data provider sends this information endorsed by its control information. Data provider pre assigned the symmetric keys and transmitted to corresponding proxies that are encrypted form. So that our method does not need any other party key agreement protocol.

2. Intermediary Proxy And Client Protocol

At some stage in content service processing, the primary proxy in each P-proxy can also delegate the content services to another proxy in the same P-proxy or execute the function by itself. The Primary proxy decides to delegate its function to another proxy q in the P-proxy, the major proxy first perform the integrity checking. In the second step if there is no error, the primary proxy send all the received packages to q. The q sends back only the updated segments with the delegate Hash attributes signed by q.

3. Recovery Prol

An easy way for the data server to broadcast the P-Proxies in the content services that the process has failed and aborted. Whenever this approach exposes the protocol to possible failures. If anyone proxy is malicious and generates the corrupted segments the entire process fails.

B. Parallel Secure Content Service Cache Proxy Protocol

When a client request is submitted to a cache proxy first it checks which may give a cache hit that is requested content is cached by the proxy.so the content is sent directly to the client without any processing. When Cache hits it can largerly reduce the communication costs for delivering and computation costs for processing. Whenever requested content is not at readly available at the cache proxy,the content proxy handles the requested as follows:

1. The cache proxy calls its access control system. If the request is denied, then the client is notified.
2. The cache proxy generates control information for the involved P-proxies and the client.
3. The cache proxy ends the control information to a data server.

IV. Conclusion and Feature Work

In this paper, we have proposed a protocol for distributed document update in cooperative systems. The protocol enforces both flow and security policies of a document and simultaneous updates on different parts of a document can be executed. We have presented a solution for secure content services characterized by a scalable and robust.

Our protocol allows a client to verify that the received data is authentic and transformations on the data are properly authorized. Our approach also assures data confidentiality during transmission. It highlights load distribution through P-proxies to improve system performance and supports parallel content services. Because no modification is required to current content distribution systems in order to adopt our approach, our work is easy to deploy for many applications. In addition, our approach is extensible; if a new type of content service is required, our architecture can be easily adapted to the new requirement. In this paper we have introduced Elliptic-Curve Cryptography (ECC) technique so that we can get scalable and robust network architecture.

For ECC, Scalar multiplication is the core operation to convert the given plain text to the cipher text. Scalar multiplication can be performed using point addition and point doubling. Point addition can be carried out with mixed coordinates to reduce the number of conversions from affine to projective coordinates. Therefore the time taken and area required to perform point addition is reduced in mixed coordinates when compared with pure projective coordinates. Point doubling is done with projective coordinates.

References

[1] Yunhua Koglin, Danfeng Yao, "Efficient and Secure Content Processing and Distribution by Cooperative Intermediaries" IEEE Tranc., Vol 19, No.5, May 2008.

[2] G. Berhe, L. Brunie, J.M. Pierson, "Modeling Service-Based Multimedia Content Adaptation in Pervasive Computing", Proc. First Conf. Computing Frontiers, Apr. 2004.

[3] C.H. Chi, Y. Wu, "An XML-Based Data Integrity ServiceModel for Web Intermediaries", Proc. Seventh Int'l Workshop WebContent Caching and Distribution (WCW '02), Aug. 2002.

[4] Extensible Markup Language (XML), [Online] Available : http://www.w3.org/XML/,2007.

[5] A. Fox, S.D. Gribble, Y. Chawathe, E.A. Brewer, "Adapting toNetwork and Client Variation Using Active Proxies: Lesson.

[6] S. Buchholz, A. Schill, "Adaptation-Aware Web Caching:Caching in the Future Pervasive Web", Proc. 13th GI/ITG Conf. Kommunikation in Verteilten Systemen (KiVS), 2003

[7] V. Cardellini, P.S. Yu, Y.W. Huang, "Collaborative Proxy System for Distributed Web Content Transcoding", Proc. NinthACM Int'l Conf. Information and Knowledge Management (CIKM '00), Nov. 2000.

[8] S. Chandra, C.S. Ellis, "JPEG Compression Metric as a Quality-Aware Image Transcoding", Proc. Second Usenix Symp. InternetTechnology and Systems (USITS '99), Oct. 1999.

[9] C.H. Chi, Y. Lin, J. Deng, X. Li, T. Chua, "Automatic Proxy-

Based Watermarking for WWW", Computer Comm., vol. 24, no. 2,pp. 144-154, Feb. 2001.
[10] L. Breslau, P. Cao, L. Fan, G. Phillips, S. Shenker, "Web Caching and Zipf-Like Distributions: Evidence and Implications,"Proc. IEEE INFOCOM '99, Mar. 1999.
[11] C. Aggarwal, J.L. Wolf, P.S. Yu, "Caching on the World WidwWeb", IEEE Trans. Knowledge and Data Eng., vol. 11, no. 1, pp. 94-107, Jan. 1999.

Satya P Kumar Somayajula is working as an Asst.Professor, in CSE Department, Avanthi Institue of Engg & Tech, Tamaram, Visakhapatnam,A.P., India. He has received his M.Sc(Physics) from Andhra University, Visakhapatnam and M.Tech (CST) from Gandhi Institute of Technology And Management University (GITAM University), Visakhapatnam, A.P., INDIA. He published 5 papers in reputed International journals & 5 National journals. His research interests include Image Processing, Networks security, Web security, Information security, Data Mining and Software Engineering.

Sesi kala Bapatla studying M.Tech SE in Avanthi Institute of Engg & Tech, Tamaram, Visakhapatnam,A.P., India. And received her B.Tech from Prakasam Engg college, Kandukur. Her research interests including Networks security, Web security, Data Mining.