International Journal of Latest Trends in Engineering and Technology
Special Issue April-2018, pp. 129-132
e-ISSN:2278-621X

SURVEY ON FLEXIBLE DATA ACCESS CONTROL BASED ON WEB BROWSER APPLICATION WITH CDN PEER- TO- PEER HYBRID ARCHITECTURE IN CLOUD COMPUTING

Ramapriya Arumugam[1], Sivamani kandan Ravi kumar[2], R. SriGokulam[3]

Abstract- Cloud Computing is a design in which assets can be spared and recovered for all intents and purposes on the virtual server with insignificant exertion over the web in an open domain. A web program has been produced utilizing some progressed scripting procedures which offers client experience and responsiveness appropriate for different stages are ending up progressively prevalent. To keep touchy client information secret against unapproved servers, utilize cryptographic techniques by giving information decoding key just to approved clients. Be that as it may, this prompts a substantial calculation workload on the information proprietor for key and information taking care of when little-grained information gets to control is wanted, and in this way don't have much movement. The Internet usage has been shifted from host-to-host centralized model to content dissemination model. The Content Delivery Network and Peer to Peer are two fundamental advances that give information construct benefits in light of the Internet. We have actualized the Http information extraction on the customer side to diminish the over-burden on the server side. The extracted information has been transmitted to the server over TCP/Ip(Stateful) as opposed to Http(Stateless) convention. Both ask for and reaction have been connected cryptographic procedures (128 piece AES) for every exchange where encryption and unscrambling are done on both customer and server side or the other way around. The decoded information will be shown on the program. We propose ID related web program with some reserving functionalities which gives a route to the substance to be scattered and to discover the closest system in ID Net having comparative substance. Inside the cryptographic component, we incorporate the idea of setting mindful confirmation and benefit assessment keeping in mind the end goal to help different control procedures. Through a profound investigation, the security and execution of our plan have been assessed. The outcomes demonstrate that our plan is adaptable and productive for information privacy of access control in distributed computing.
Keywords—Cloud computing; access control; CDN; Peer- to- Peer; Http; AES encryption decryption; TCP/IP

1. INTRODUCTION

Cloud computing is a rising innovation in which calculation of assets framework is given in a shape of administration over the Internet. In cloud computing, there is no compelling reason to think about the area and the arrangement of the framework which gives the administration. The cloud empowers the server farm to work like the web and process the assets to be gotten to and shared as a virtual asset in a safe and way. The fundamental qualities of mists are versatility, homogeneity, virtualization, minimal effort programming, secure access, geographic dispersion. Distributed computing organization models are of three kinds: private, open and mixture. General society cloud powerfully assigns assets in view of client premise through web applications. The private cloud gives security to workers and clients of an association. Though in the Hybrid cloud which is the blend of Public cloud and private cloud. In this sort of cloud benefits, the inner assets are made under the control of the client and outer assets are conveyed by a cloud benefit provider(CSP). The web application has been created where it delivers the responsive website page. The web application is of two sections customer and server. The customer shows the web structure characterized by HTML substance and CSS alongside JavaScript. For the most part in a customer service where the customer asks for takes excessively to react keeping in mind the end goal to diminish the time and utilize it productively CDN and Peer to Peer are utilized. Content Delivery Network(CDN) is a gathering of servers that convey page and web substance to the client in light of the client's area, the source of the site page. CDN will scan for the closest server and store the imitations of an every now and again got to page and give that substance to the client. Associate to-Peer(P2P) is a system of PCs where each companion goes about as a customer and server for sharing assets between them. The Http ask for of the page to be seen is removed from the customer side keeping in mind the end goal to diminish the over-burden of the server. The extricated information is changed into TCP/Ip organize. TCP/Ip is utilized for a dependable transmission of information and furthermore recovers the site page fastly. For security reason encryption and decoding is done on both customer and server side. The current framework isn't adequate to guarantee the security of clients. The proposed approach is utilized a cryptographic system, for example, AES (Advanced Encryption Standard) calculation to scramble the separated information for the security concerns.

[1] Final year UG student, Department of CSE, Meenakshi Sundararajan Engineering College, Kodambakkam, Chennai, India
[2] Final year UG student, Department of CSE, Meenakshi Sundararajan Engineering College, Kodambakkam, Chennai, India
[3] Assistant professor, Department of CSE, Meenakshi Sundararajan Engineering College, Kodambakkam, Chennai, India

The rest of the paper is organized as follows. Section 2 presents an overview about data access control on cloud. Section 3 gives an idea about how data is extracted on client side. Section 4 depicts encryption and decryption of data. Section 5 gives an outline of CDN and Peer-to-Peer usage on cloud. Section 6 concludes the work.

2. DATA ACCESS CONTROL ON CLOUD

The individual information put away in the Cloud are typically encoded and their entrance has been controlled. Be that as it may, this information ought to be gotten to by different substances keeping in mind the end goal to satisfy the cloud benefit. How to control the entrance of this information is the principle issue? In [1] the information proprietor should control the access of information. In order to avoid this, the information proprietor does not know how to control the entrance to information. Keeping in mind the end goal to stay away from that Access Control List (ACL)have been utilized for secure information access in the cloud where every client will be given consent and degree. At first, the information proprietor indicates an ACL for the information and after that encode the information with the symmetric key, which is scrambled with general society key of the client's in the Access Control List. Thus, just the clients of that ACL can recuperate the first information utilizing their private keys. The primary disadvantage is that the cost for encryption is bigger relying on the quantity of clients in the ACL.

In [2], Discretionary access control is traditional access control model where a group of users set different access rights to different objects provide authority to users and support the audit.

[3][4][5] [6] Another access control technique on secure cloud computing is Role-Based Access Control(RBAC) where it provides flexibility to an organization's policy and structure. RBAC have certain policies which are enforced by Role-Based Encryption(RBE) where the users with the roles specified by the RBAC can encrypt and decrypt the data.

3. EXTRACTION ON CLIENT SIDE

The extraction is done on the client side mainly to reduce the burden of server. Because server receives more request and it takes too much to respond. In order to avoid that extraction process have been introduced.

In [7] information extraction, the initial step is to recover contribution from the customer in sense pick the HTML code that we should center around while out of sight the application will follow the execution of information stream has been finished. At that point reinterpret a similar information and the conditions are followed with the application execution follow as a rule. At the point when the translation achieves a specific point then the progressions are made in the HTML code. After the progressions are done code with appropriate substance are held while the undesirable substance has been sifted and shown in the web program with the reasonable use situation. Fig1.0 The below diagram specifies the flow of how the data have been extracted.

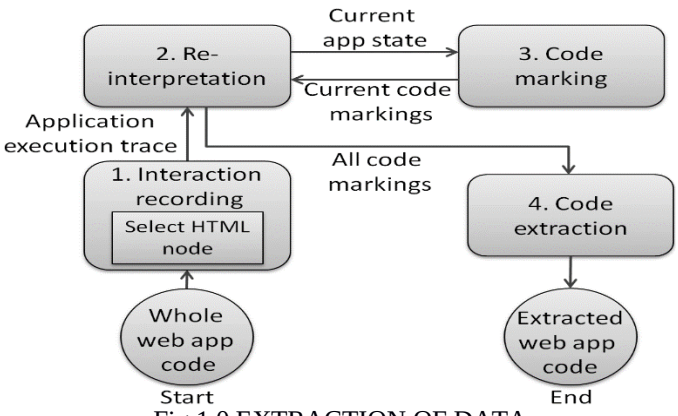

Fig 1.0 EXTRACTION OF DATA

4. ENCRYPTION AND DECRYPTION

In a cryptographic framework for ensuring the information, DES calculation was presented which was significantly more grounded than other cryptographic methods. DES utilizes a similar key to encode and unscramble the information so both the sender and the collector must know and utilize an indistinguishable private key from well. In any case, the time required for cryptanalyst has been reduced on the grounds that the innovation has been created quickly. Henceforth DES might be assaulted by different cryptanalysis utilizing some parallel procedure.

In [8], Encryption methods have been connected to guarantee the wellbeing and security of information in the cloud in a private way. Among the cloud concerns, for example, honesty, youthfulness, cost, execution, security and protection and uptime the major and essential one is security and protection. The security issues should have been considered and settled on the grounds that they are the significant prevention to going up against the cloud condition. The moved toward models are Rijndael Encryption Algorithm and Extensible Authentication Protocol. The later one is a piece figure mechanism(AES) where it contains four conditions of round tasks, for example, Substitute bytes, move lines, include round key, and blend

segments with key sizes, for example, 128bit (10 round) or 192(12 round) or 256(14 round) piece which we can pick as indicated by our need. Lamentably, the unapproved client got the scrambled information likewise he can't unscramble the information. The later in which parameters and keying materials are utilized and transmitted with the assistance of Challenge-Handshake Authentication Protocol (CHAP) which gives the best approach to validation. The issues in verification and approval have been overwhelmed by this handshake system.

In [9], to guarantee security worry of delicate information, the most top to bottom activities were allotted to the information proprietors. This prompts computational overhead on proprietor side. Alternate issues are the Cloud server can't approve the client information for information secrecy and the other issue is full control of assets were not physically on the customer side. The answer for this issue is to scramble the information on the cloud server with key and Communicating the unscramble key with the trusted clients as it were. The present arrangement is the Access control List(ACL) per record get to. Indeed, even here and there documents been grabbed into single record bunch for quicker access and recovery. Be that as it may, the complexity of this plan is that ACL is straightforwardly identified with the quantities of clients in the Cloud Server.

In [10], cloud computing is an infrastructure where the user can access their data from any machine over the internet. Users after transmitting the data to the server, he should take consideration whether the data have been stored in a secured manner. To ensure this data should be encrypted on both client and server side. The drawbacks of the system are no authorization for accessing the cloud, no authorization for resources, not account the time taken for encryption. To provide the way for secure data access the proposed technique is AES Algorithm to be applied on the client side. They consist of three keys such as the private, public and symmetric key. The both private and public were used for encryption and decryption on the client side. The cloud server stores the encrypted data. Symmetric key has been used to generate secret key through which the encryption and decryption of data or file have been taken place on the client side only. It is applicable all data formats such as audio, video, text and so on.

5. CONTENT DELIVERY NETWORK AND PEER TO PEER

In [11], On the off chance that the client asked for information to be conveyed from the source server the reaction time will be higher. The substance conveyance organize has been utilized to convey the substance to the end clients in a short reaction time with the assistance of edge servers. The edge servers are where they have the reproductions or a few substances identified with the area from the starting point server. What's more, the CDN absorb the steering for the customer to achieve the best edge servers as indicated by their Geographical area. The significant favorable position of CDN is that it aces the issues like system Congestion, arrange disappointments and fundamentally needn't bother with an Infrastructure to give content conveyance to the substance suppliers. The rising distinctive kind of CDN is P2P (Peer to Peer) CDN.

Shared is the Distributed framework which contrasts from conventional customer/server show. It depends on the Servant based engineering where workers involve both the customer and server. It isn't a concentrated framework. The P2P is of two sorts, Hybrid P2P and Pure P2P. Half and half P2P contains super companions (Specialized associates) through which different companions can pick up information about their comparing associates to impart the information assets to peers. The super servers have the snippets of data, for example, ordering, Network Configurations, seeking and companion finding. The other one is unadulterated P2P where there are no any super companions, each associate is dealt with similarly. It utilizes the overlay conventions for conveying between peers. These days they are utilizing TCP, UDP, and HTTP over Internet Protocol. The upsides of the P2P-based designs incorporate dynamic data archives, content-based tending to, high adaptation to non-critical failure, accessibility by means of repetition, upgraded stack adjusting, and enhanced hunts.

Table 1.Comparative Analysis

Factors /Algorithms	DES	AES
KEY SIZE	56 bit	128,192 or 256 bits
CIPHER TYPES	Symmetric block	Symmetric block
RESISTANCE ANALYSIS	Vulnerable to differential and linear	Strong against differential and linear
BLOCK SIZE	64 bits	128 bits
ROUNDS	16 rounds	10,12 or 14 rounds
SECURITY	Inadequate	Strong enough

Table 2. Comparative Analysis

Protocol /Protocols	HTTP	TCP/IP
LAYER	Application layer	Network layer
COMMUNICATION SERVICES	As series of sessions	Intermediate level between application program and Ip
NATURE	Stateless protocol	Reliable protocol

6. CONCLUSION

In the survey, we have reviewed different papers that uses different cryptographic algorithms to fortify secure data Integrity. Since the efficient security has been provided by the AES algorithm. The HTTP information extraction has been done on the client side to scrap the undesirable information and just the crude information has been transmitted to the cloud server. With a specific end goal to guarantee information security and trustworthiness, the proposed approach is AES calculation for encryption and unscrambling on both customer and server side. For a reliable transmission, the scrambled crude information has been sent as a TCP ask for to the cloud server, where the demand has been decoded and handled to get the reaction. The reaction information has likewise been scrambled and transmitted over TCP reaction to the customer in an approach to accomplish information security. The information will be unscrambled on the customer side and showed on the web program. There will be two Queues– IN queue and Out queue. In queue storesthe request till it's been transmitted. Out queue stores the received response from the server. After the session end, the records in the out queue been erased. This kind of approach will decrease the underload on the customer side and over-burden on the server side. There will be the most extreme use of CPU on the customer side and least process is just done on the server side. The data Centers have been expanding because of the over-burden on the server. This proposed approach will limit the requirement for the server farm. The safe and solid transmission of information can be accomplished through this approach.

7. REFERENCES

[1] E. Goh, H. Shacham, N. Modadugu, D. Boneh, “Sirius: Securing remote untrusted storage”, Proc. of NDSS, 2003, pp. 131–145.

[2] Jun Hu, Lei Chen, Yunhua Wang, Shi-Hong Chen,” Data Security Access Control Model of Cloud Computing”, International Conference at Computer Sciences and Application on 2013.

[3] Niteen Surv, Balu Wanve, Rahul Kamble, Sachin Patil,” Framework for Client Side AES Encryption Technique in Cloud Computing”, IEEE International Advance Computing Conference (IACC),2015.

[4] L. Zhou, V. Varadharajan, M. Hitchens, “Achieving secure role-based access control on encrypted data in cloud storage”, IEEE Trans.On Information Forensics and Security, vol. 8, no. 12, pp. 1947-1960, 2013.

[5] W. Wang, J. Han, M. Song, X. Wang, “The design of a trust and role based access control model in cloud computing”, in Proc. of 6th International Conference on Pervasive Computing and Applications,2011, pp. 300-334.

[6] S. Yang, P. Lai, J. Lin, “Design role-based multi-tenancy access control scheme for cloud services”, Proc. of International Symposium on Biometrics and Security Technologies, 2013, pp. 273-279.

[7] Daniel Pakkala and Juhani Latvakoski,” Towards a Peer-to-Peer Extended Content Delivery Network”.

[8] Sanjoli Singla, Jasmeet Singh,” Cloud Data Security using Authentication and Encryption Technique”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, July 2013.

[9] V. Sathya Preiya, R. Pavithra, Dr. Joshi,” Secure Role based Data Access Control in Cloud Computing”, International Journal of Computer Trends and Technology- May to June Issue 2011.

[10] T. Zhu, W. Liu, J. Song, “An efficient role based access control system for cloud computing”, Proc. of IEEE CIT2011, 2011, pp. 97-102.

[11] Josip Maras, Jan Carlson, Ivica Crnkovic,” Extracting Client-Side Web Application Code”, International World Wide Web Conference Committee(IW3C2), April 2012.