International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-5, March 2020

Efficient and Secure Data Transaction with Storage Optimization in Information Centric Network

S. Sakthivel, S. Hemalatha

Abstract: ***Network utilization has been widely utilized by means of greater wide variety of users and managing user request with its increasing demand for content material transport is an main task has been dealt with by using Information centric network (ICN) through network cache method. An efficient access manage mechanism is required to make use of community resource, content material dissemination and better delivery service. Cache primarily based records shipping is an environment friendly approach to handle improving users request however it reasons high computation overhead and surprising extend in statistics delivery. In our proposed work an environment friendly method to beautify the utilization of network, request dealing with and storage optimization has been bought via Secure and Efficient Resource Utilization Framework (SERUF) for ICN. Unauthorized consumer request has been validated and blocked in edge of the community itself and cache based totally statistics retrieval is applied with content de-duplication. To maintain our file in impervious way thru Enhanced Attribute based encryption (E-ABE) is used which lets in special file to save in server. Hence our strategy consists of storage utilization, secure information retrieval and handles user request in efficient way.***

Keywords: An efficient access manage mechanism is required to make use of community resource, content material dissemination and better delivery service.

I. INTRODUCTION

Information Centric Network:

The ICN targets to shift the current complex Internet model to a simple and established one. The basic networking unit is never again the perceived hub (servers, switches, terminals). The ICN organizing activities are completely founded absolutely on the named content targets. ICN is collector driven systems administration model, where end-clients exclusively straight out their inclinations for a given substance, the total network is accountable for directing the solicitations dependent on the substance names toward the fine substance material holders and turning in the substance through the invert ways to the end-clients. The ICN goals to build the highlights quickly into the systems administration structure. It locally comprises of the angles as area free naming, name-based steering, in-systems administration storing, local multicast, self-made sure about substance, and so forth. Information Centric Network (ICN) is a kind of network shape which is insights driven on the other hand than have driven, for example right now organize more prominent criticalness is given to the substance being continued system as opposed to from where the substance is removed. In inheritance systems content is conveyed from beginning spot servers, anyway here in ICN it's currently not basic that content material to be conveyed from starting point servers, it tends to be conveyed from some place in the network since this substance is locale free.

Introduction of in-network caching function in ICN allows the routers to store content in their content material store, when a request arrives for a particular content, router assessments whether or not the content material is available in its store, if it is reachable then router responds to that request via sending content back to the requester.

Issues in ICN:

The cache pollution assault goals a switch's substance material area with the goal of modifying its arrangement of stored content material following in an expansion in the recurrence of substance retransmission, and diminished system goodput.

Due to ICN's help for unavoidable storing, content material articles can be repeated at some phase in the system. Despite the fact that this strikes content shut to the part and helps limit network burden and substance recovery inactivity, it comes at a worth distributers lose oversee over these stored duplicates and can't referee get to. Consequently, there is need for proficient get right of passage to control, which permits reuse of cached content and prevents unauthorized accesses.

Objective of our work:

- To attain maximum performance by utilizing resources efficiently.
- To avoid de-duplication content for storage optimization.
- To prevent unauthorized user access in the beginning stage itself.
- Secure data storing and retrieval of data.

II. LITERATURE SURVEY

Nikos Fotiou and George C. Polyzos (2016), depicts Traditional types of encryption present great measured overhead with regards to offering substance to huge and dynamic organizations of clients. To this end, intermediary re-encryption bears an advantageous arrangement. Right now, use Identity-Based Proxy Re-Encryption (IB-PRE) to supply secrecy and get passage to control for content things shared over ICN, acknowledging impervious substance material dissemination among dynamic arrangements of clients.

Revised Manuscript Received on March 30, 2020.

* Correspondence Author

***Dr. S. Sakthivel** Ph.D, Professor, Department of Computer Science and Engineering , Sona College of Technology, Salem.

S. Hemalatha M.E, Department of Computer Science and Engineering, Sona College of Technology, Salem.

In qualification to practically identical IB-PRE based arrangements, our chart permits every shopper to create the framework parameters and the mystery keys required by methods for the underlay encryption plot the utilization of their own Private Key Generator, thusly, our technique does never again experience from the key escrow issue. Also, our arrangement further loosens up the trust necessities on the capacity hubs by keeping them from imparting usable substance material to unapproved clients.

Bing Li et.al (2016), another system building that goals to vanquish the deficiency of current IP based frameworks organization structure. Instead of sifting through a relationship between the giving has, ICN bases on the substance, for instance data, transmitted in organize. Content copies in ICN can be put away at uncommon regions. The substance is out of its owner's control once it is conveyed. Thusly, completing get right of entry to direct security plans on spread substance material copies is essential in ICN. Characteristic Based Encryption (ABE) is a potential framework to put into effect such control instruments at this moment. In any case, applying ABE in ICN faces two troubles: from the board perspective, it is itemized to control properties in regulated propensities; from privateness security, disdain in like way arranges, the maintained substance get right of section to insurance approaches are available to all the ICN customers. Along these lines, it is faultless that unapproved content watchers are as of now not prepared to recuperate the passageway approach. To this end, an insurance sparing addition section to control plan for ICN and its looking at property association answer are shown.

Qi Li et.al (2015), presents Several Information Centric Network (ICN) structures have been proposed as contender for the future Internet, intending to cure various notable difficulties in the contemporary IP-based Internet design, for example, versatility, content material dispersal and multi-way sending. When all is said in done, security and protection are viewed as basic necessities in ICN. In any case, current ICN plans need developed in privateness assurance for content material suppliers, e.g., any switch in an Internet Service Provider in ICN can store any substance, which may furthermore final product in data spillage. Right now, advocate Mandatory Content Access Control (MCAC), a designated realities drift control instrument to permit a substance organization (CP) to control which arrange hubs can reserve its substance. In MCAC, a CP characterizes distinctive insurance names for explicit substance, and substance switches investigate these marks to decide whether a substance object must be stored.

Gergely Acs et.al (2017), talks about ICN is a developing systems administration worldview where named and routable data (content) is the central point.Users send explicit solicitations (interests) which indicate content with the guide of name, and the system handles steering these interests to some element equipped for pleasant them with the breathtaking data reaction (maker). One key capacity of ICN is sharp in-arrange content material storing. This property encourages effective substance appropriation through diminishing data transmission utilization, decreasing system clog, and improving the substance recovery dormancy by methods for clients (buyers). Lamentably, the indistinguishable capacity is also hazardous to privateness of substance clients and makers. Easy to execute, and testing to identify, timing assaults can exploit ICN switches as "prophets" and license a foe to examine whether a close by buyer of late mentioned certain substance. The assault use a planning side channel that relies upon switch stores and is applied through mentioning a couple of parcels from each bit of substance material being examined. So also, testing ambushes that target content material makers can be utilized to see if or not positive substance material has been nowadays dispersed.

Daojing He et.al (2011), depicts a dispensed get passage to oversee module in remote sensor systems (WSNs) endorses the network to approve and supply client get right of section to benefits for in-arrange information get to. Earlier query typically centers around planning such get right of section to control modules for WSNs, however little consideration has been paid to ensure client's distinguishing proof privateness when a client is built up by means of the system for records gets to. Frequently, a buyer does now not lean toward the WSN to buddy his character to the realities he demands, extraordinarily in a solitary proprietor multi-client WSN.

III. PROPOSED SYSTEM

get admission to oversee from content material arrangement, we will in general let switches at the network side guarantee clients' solicitations all together that the data measure and store resources inside the system territory unit just available to authorized clients. For privateness security, clients affirm themselves through assembling a real bunch mark to deal with them mysterious to the domain switches. all things being equal, signature innovation and confirmation need expensive calculation. In this way, a trifling answer that utilizes signature on each and each solicitation is unreasonable. to remain expelled from the critical development, SERUF utilizes the progression of clients' solicitations and extensions hash chain approach with group signature all together that lone the essential of a lot of solicitations needs signature activity and furthermore the rest might be implies that of light-weight hash activity.
Since the lengths of hash chains area unit a similar because the numbers of users' requests, signatures and hash chains may be used as service credentials to convert content material vendors that ISP actually offers the supplier it claims. In addition to this duplication in server will leads to time consumption in searching process. As we be aware of already, cache is transient reminiscence which has minimal storage therefore utilizing it environment friendly way is mandatory. Therefore in our proposed in addition to efficient authentication technique we are going to pick out reproduction detection based on content. While figuring out content based totally duplication will automatically will increase storage utilization hence this will leads to efficient storing and retrieval of facts in cache. Hence the performance of our device will be enhanced compared to current method.

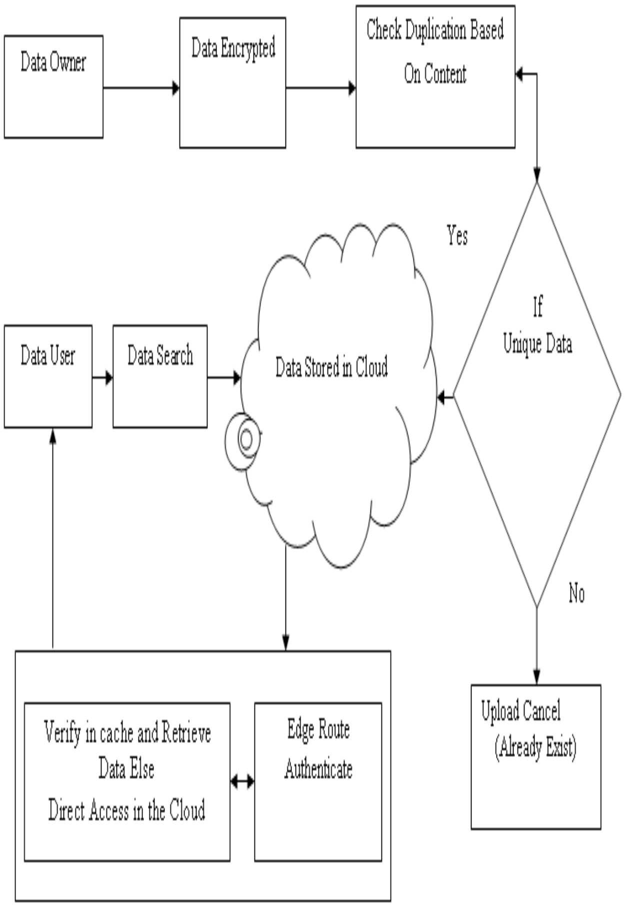
Data Owner
Data Encrypted
Check Duplication Based On Content
Yes
If Unique Data
Data User
Data Search
Data Stored in Cloud
No
Verify in cache and Retrieve Data Else Direct Access in the Cloud
Edge Route Authenticate
Upload Cancel (Already Exist)

Figure 1: overall system architecture

Step 1: The facts owner wishes to outsource the information into cloud for comfort of records sharing. The data proprietor is in cost of encrypting information for a set of receivers. Initially proprietor wants to register their details to create an account. Once consumer registered efficaciously he/she may also login and upload the data. Cloud is not totally secured therefore data owner want to encrypt the statistics for ensuring security. Here E-ABE is used to encrypt the statistics in cloud. Data proprietor wishes to add or submit his content material to the cloud server, so that clouds users can execute queries to search the information. Data proprietor believes and trusts solely the relied on users. Data owner has set of unique attributes, and a key, which can be used for records accessing.

Step 2: File uploaded by way of proprietor is saved in cloud. Large quantity of users will add data in cloud for further processing there is risk for storing of same file in cloud which is represented as duplication. Many methods are on hand to discover duplication in our gadget content primarily based duplication verification is deployed. In general with some specific parameters information duplication will be identified such as file name, dimension and type this attains a positive degree of result. In our proposed we become aware of duplication based on file content. If equal content material is on hand with exceptional parameters are also efficiently detected and uploaded in cloud. Hence this method identifies duplication and stores in cloud efficaciously and it saves storage and query processing.

Step 3: User will search documents transmitted from supply (data owners) to destination (cloud) via keyword search. Initially user needs to create an account in cloud to get right of entry to the facility furnished in it. Once person login the machine efficiently person will search the file by way of dint of keyword. Based on key-word ciphertext uploaded in cloud will be shown and user can request the required file. The cloud customers required authentication to get right of entry to the facts or record. Reliable user's account ought to be handy in cloud. If it is not, then they should register first. Hence, user can enter authenticated key and search the content. Keyword search technique is generally used for searching unstructured data. With time it has resulted in development of number of strategies of ranking and ranking of question results and to estimate the effectiveness of those techniques. Keyword search techniques are very useful for examining both the structured as properly as the unstructured information which consists of the large quantity of the textual information. By using Keyword Search person can post key-word to search engines (Internet Search) or structured information and in flip it returns a list of files to person in accordance to ranking.

Step 4: While processing two consumer question Initially authentication manner will take location the edge router verifies whether the consumer is licensed or not. Once the verification process was done the request will be demonstrated from the cache enabled router. If the statistics is on hand in cache it will retrieve it and returns to consumer otherwise it will search in the server. Therefore records will be processed efficaciously as nicely as effectively.

ABE:

Attribute - based encryption (ABE) is a public – key algorithmic rule supportede to several ciphenions that permits users to encrypt and decode information based on user attributes. In their context, the role of the parties is taken by the attributes. Thus, the access structure can contain the licensed sets of attributes. They limit the eye to monotone access structures. However, it's conjointly potential to comprehend general access structures mistreatment the techniques by having the attribute as a separate attribute altogether. Thus, the quantity of attributes within the system are doubled. From currently on, unless declared otherwise, by associate access structure we have a tendency to mean a monotone access structure.

There are four algorithms in a CP-ABE scheme:

(1) Setup: it takes security parameters as input and outputs public parameters PP and master secret key MSK.

(2) KeyGen: it takes public parameters PP, master secret key MSK, and a set of attributes S as input and outputs secret key SK_S corresponding to S.

(3) Encryption: it takes public parameters PP, access policy W, and message M as input and outputs the ciphertext CT_W.

(4) Decryption: it takes public parameters PP, ciphertext CT_W, and secret key SK_S as input and outputs the message M, if and only if the attributes S satisfy the access policy W; i.e., $S \vDash W$.

IV. RESULT AND DISCUSSION

In network, resource allocation is an critical issue for attaining better performance. To process user request efficiently cache based processing is used similarly security has been implemented through E-ABE. Hene this session shows our performance result in graph.

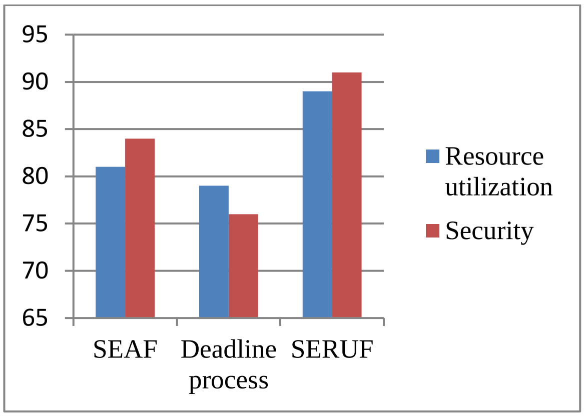

Figure 4.1 parameter comparion graph

The above graph shows parameter comparison such as resource utilization and security. It shows our proposed method achieves better result compared to other available existing methods.

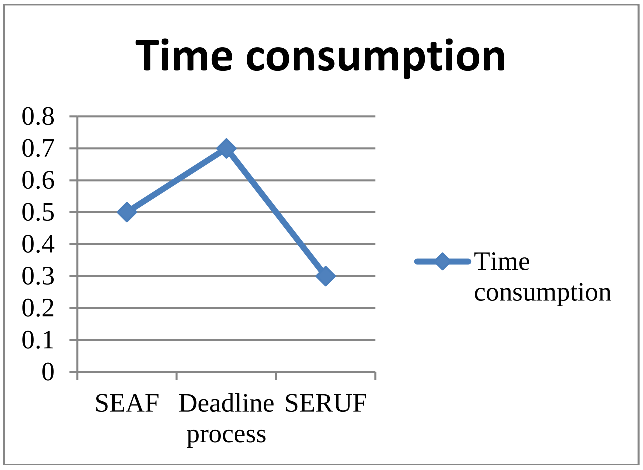

Figure 4.2: Time consumption

Compared to other methods our proposed work achieves minimum time consumption and it increases performance of the system. Through cache based processing efficient query response will be obtained from server and storage will be optimized effectively.

V. CONCLUSION

Secure and Efficient Resource Utilization Framework (SERUF) was introduced in our work. ICN has becoming an emerging technology and to handle issues is focused and solved. Cache based data retrieval is an efficeint method to process huge number of request from various users. In order to increase system performance, storage uilization has been focused. There is a possibility for redudant data availability in storage which can be reduced by E-ABE which encrypts content to be uploaded and generate hash value. Based on this hash value duplication of similar file was identified accuately and avoided. Through encryption process if any unauthorized user accessing is not possible. Hence it concludes that secure data sharing and efficient resource utilization was done through cache based services. Compared to existing method our method acheives better result and increases network performance. Our security analysis and experimental results demonstrate that SERUF is a promising solution for the access control in ICN, which meets various security requirements and also guarantees good enough efficiency.

REFERENCES

1. V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, “Networking named content,” in Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies (CoNEXT 2009). ACM, 2009, pp. 1–12.
2. K. Xue, T. Hu, X. Zhang, P. Hong, D. S. Wei, and F. Wu, “A withered tree comes to life again: Enabling in-network caching in the traditional IP network,” IEEE Communications Magazine, vol. 55, no. 11, pp. 186– 193, 2017.
3. Q. Li, P. P. Lee, P. Zhang, P. Su, L. He, and K. Ren, “Capabilitybased security enforcement in named data networking,” IEEE/ACM Transactions on Networking, vol. 25, no. 5, pp. 2719–2730, 2017.
4. E. G. AbdAllah, M. Zulkernine, and H. S. Hassanein, “DACPI: A decentralized access control protocol for information centric networking,” in Proceedings of 2016 International Conference on Communications (ICC 2016). IEEE, 2016, pp. 1–6.
5. N. Fotiou, G. F. Marias, and G. C. Polyzos, “Access control enforcement delegation for information-centric networking architectures,” in Proceedings of the 2nd Edition of the ICN Workshop on Information-Centric Networking. ACM, 2012, pp. 85–90.
6. N. Fotiou and G. C. Polyzos, “Securing content sharing over ICN,” in Proceedings of the 3rd ACM Conference on Information-Centric Networking (ICN 2016). ACM, 2016, pp. 176–185.
7. S. Misra, R. Tourani, F. Natividad, T. Mick, N. E. Majd, and H. Huang, “AccConF: An access control framework for leveraging in-network cached data in the ICN-enabled wireless edge,” IEEE Transactions on Dependable and Secure Computing, Avaliable online, 2017, https://doi.org/10.1109/TDSC.2017.2672991.
8. Q. Li, X. Zhang, Q. Zheng, R. Sandhu, and X. Fu, “LIVE: lightweight integrity verification and content access control for named data networking,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 2, pp. 308–320, 2015.
9. B. Li, D. Huang, Z. Wang, and Y. Zhu, “Attribute-based access control for ICN naming scheme,” IEEE Transactions on Dependable and Secure Computing, Avaliable online, 2016, https:// doi.org/10.1109/TDSC.2016.2550437.
10. M. Mangili, F. Martignon, and S. Paraboschi, “A cache-aware mechanism to enforce confidentiality, trackability and access policy evolution in content-centric networks,” Computer Networks, vol. 76, pp. 126–145, 2015.