International Journal of Advanced and Innovative Research (2278-844)/

Volume 7 Issue 11

Trust Enhanced Cryptographic Role Based Access Control if Secure Cloud Data Storage

[1]Sushma Uopanaboina, [2]B Anand Kumar

[1]Research Scholar, [2]Assistant Professor, Department of Computer Science & Engineering

KODADA Institute of Technology & Science For Women, Kodad

Abstract: Cloud data storage has provided significant benefits by allowing users to store massive amount of data on demand in a cost-effective manner. To protect the privacy of data stored in the cloud, cryptographic role-based access control (RBAC) schemes have been developed to ensure that the data can only be accessed by those who are allowed by access policies. However, these cryptographic approaches do not address the issues of trust. In this paper, we propose trust models to reason about and to improve the security for stored data in cloud storage systems that use cryptographic RBAC schemes. The trust models provide an approach for the owners and roles to determine the trustworthiness of individual roles and users, respectively, in the RBAC system. The proposed trust models consider role inheritance and hierarchy in the evaluation of trustworthiness of roles. We present a design of a trust-based cloud storage system, which shows how the trust models can be integrated into a system that uses cryptographic RBAC schemes. We have also considered practical application scenarios and illustrated how the trust evaluations can be used to reduce the risks and to enhance the quality of decision making by data owners and roles of cloud storage service.

Keywords:-Role-based access control, trust model, cryptographic RBAC, secure cloud data storage.

1. INTRODUCTION

In today's Information Technology age, mainframe networks are usually used to share information and to converse with others. The chances of compromise the information being transferred over the networks are growing. Vulnerable data is required to be protect from illegal access from transmit over anxious and timid networks for instance Internet. Protection measures during transmit of data has turn out to be one of the hard challenge in excess of the networks. To deal with the information security issues Cryptography is one of the techniques. It is based on encryption and decryption algorithms for safe broadcast of data over the network. It is technique that has been used about thousands of years for keep the data secure from others. These days present cryptography techniques are used to give safety measures which uses mathematics techniques and based on two essential components: Algorithm and a key used to set up the algorithm operation. This present cryptographic way aim is to attain the sanctuary goals such as data secrecy, data dependability, non-repudiation and confirmation. Using the mainframe networks for transfer the acknowledgment card information, transfer electronic identification, online shopping, etc. Cryptography is a capable method that uses encryption and decryption to safe the data from prohibited admittance. To protect dependability and separation of data, encryption and decryption methods are used.

The plaintext is the unique form of data and the cipher text is the encrypted form of data. An input is a part on the basis of which information is determined. Decryption technique acquires the set text (encrypted form of data) and exchange it into plain text (original form of data) based on algorithm using a key input.

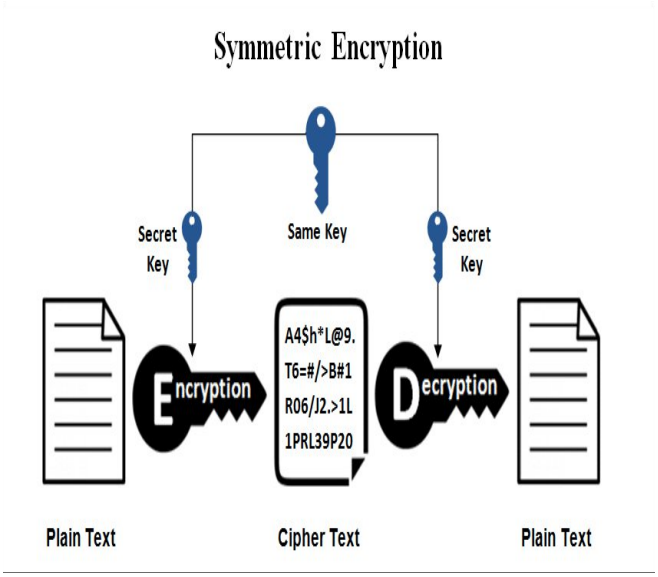

Figure 1.1: Symmetric Encryption.

Cryptography

Cryptography is a performance that secures the information from unauthorized access. Encryption algorithms and key are the basic components of cryptography. The simple text is transformed into encoded text (encrypted form) using an encoding algorithm known as encryption method. The coded text is transformed into original text using a decoding algorithm known as decryption method.

TPA (Third Party Authentication)

A TPA may be characterized as a believe admirable professional that gives us a organize to perform believe at the cloud scheme and the TPA is playing out the estimation to the cloud and playing out the client assert get entry to to able to get well the reputability comes about on the data available using the cloud, the TPA is usually a specialist that is loyal to receive the call for and convey the opinion ,generally its successive the call for – opinion approach preserve the top objective to return get advantages within the suggest integrity approval design .a remarkable most popular point of view of our design will be the cloud specialist management can be offering the capacities that have been given respectively traditional interloper auditor and perform it trustful. So it correctly diminishes the Constitution's resourceful high quality in Cloud Computing, so attending TPA-an interloper analyst that bears trustful recognition for user to implement their information security in distributed computing structure.

2. LITERATURE REVIEW

Soumya Parvatikar, Puja Prakash, Richa Prakash, Pragati Dhawale, S.B. Jadhav [1]

Private well-being document (PHR) is in most cases noticeable as a patient-pushed model of sharing well-being related expertise. But protection is the prime concern while storing data in an outsourced atmosphere. If the full entry of the PHR information is supplied to the patients that simply waste for him to preserving that knowledge. However there are disorders like dangers of the security introduction scalability in the key management and many others are the difficulties in delivering a nice-grained service to the consumer and provide a cryptographically approved provider. To provide a great-grained and comfortable access manage, an ABE (Attribute founded Encryption) service is used to encrypt sufferers knowledge. In that no longer handiest a at ease mechanism is provided but additionally provide a high-quality grained carrier and partition the patients data into various protection domains. That reduces the complexity in the administration. A cozy framework to share sufferer's information over the outsourcing environment is furnished, that helps to share patients PHR knowledge over the internet, which can be used within the therapy of the various ailments. A comfortable world access is furnished to the opposite users like doctors to uses this data for the remedy of the illnesses.

Saipavan Konda, Niranjan Reddy P [2]

Personal wellness report (PHR) is sufferer pushed model of individual wellbeing records sharing, which is commonly outsourced and put into the 0.33 occasion server, for example, cloud provider. There is among the biggest safety considerations, in view that personal health documents are saved in 13 occasion server in the untrusted atmosphere. Consequently there may be various cryptography strategies can be used to encrypt that information before outsourcing it. That provides patients a manage over the access of their information. A sufferer driven mannequin and an entry control framework to preclude unauthorized entry for the PHR knowledge. An Attribute based encryption process and a One Time Password (OTP) centred technique is used to furnish better performance to relaxed outsourcing of the information. Dynamic entry manipulate framework is provided to the patient for secure outsourcing to their knowledge.

A.Yoshitaka,S.Chujyou,H.Kato [4]

Japan is likely one of the countries where way forward for nation is probably the most raised in the world. Not handiest bettering the social medication services but additionally improving in social wellbeing care protection framework, person actions within the social services and many others. Thus PHR (individual wellness record) of the every sufferer can be used to provide expertise about the diseases which used to medication or in treatment of those ailments. Wellness knowledge evaluation is performed to furnish higher information in regards to the health care data. That digital health care data can be used through the general population to and the medical authorities to fortify the wellness care offerings. But when put that knowledge available to the general population can be cause serious protection difficulty for the patients personal data. A appropriate administration and management is required to furnish a secure entry for that information.

C. J. Wang, X. L. Xu , D. Y. Shi , W. L. Lin [5]

As a rising patient-driven mannequin of wellness information sharing, cloud-centered individual health file (PHR) framework holds top notch assurance for enticing patients and guaranteeing more compelling conveyance of medicinal offerings. A novel sufferer-driven cloud-based comfy PHR framework, which allows patients to soundly retailer their PHR information on the 13 get together cloud server, and above all share their PHR information to an broad form of customers, together with medical services supplier like doctors and attendants, loved ones or companions. To cut back the important thing administration multifaceted nature for doctors and purchasers, we partition the customers within the cloud-based PHR framework into two safety areas named open space and individual area. Now not the identical as past Cloud-based PHR framework, PHR owners scramble their PHR knowledge for common society space utilizing determine content procedure property situated encryption plan, even as they encode their PHR expertise for the man or woman area making use of mysterious multi-recipient personality centered encryption plan. Simply approved purchasers whose qualifications fulfil the predefined figure content material procedure or whose personalities fit in with committed characters can decode the encoded PHR understanding, where figure content material association or committed personalities are inserted within the scrambled PHR understanding. Vast investigative and exploratory results are exhibited which show the patient-driven cloud-based comfortable PHR framework is comfortable, versatile and productive

P. Van Gorp , M. Comuzzi [6]

Individual well-being records (PHRs) have to stay the lengthy lasting property of sufferers and must be showable to the licensed customers or like doctors and different healthcare authorities. In present situation PHR makes a speciality of the ordinary information sharing corporations and provide international healthcare framework. My PHR computing device, a sufferer- pushed mannequin is provided, that presents a more desirable framework wellbeing records sharing. In that procedure not most effective the scientific understanding but in addition related expertise to that programming of PHR is also shared. In that procedure knowledge shared over the cloud which can be utilized with the aid of the various customers. Sufferers can access the information by the use of faraway virtual desktop. Deep rooted PHR information is offered to the patients, medical professionals, coverage businesses and many others. To get viable options for the illnesses.

WB Lober, B Zierler,AHerbaugh, SE Shinstrom, A Stolyar, EH Kim, And Y Kim [7]

Personal wellness documents (PHRs) are methodology to make patient centric health offerings. There is some work is required to furnish better wellness care offerings to the patients at house and difficulties in work procedure like have an effect on of the access of these records, psychological influence, physical have an impact on etc. The results of these healthy evaluation is used by the quite a lot of companies to furnish better health care offerings to the sufferers. That help in growth of the healthcare offerings and get to the bottom of the issues of the sufferers related to the well-being care services.

3. PROBLEM IDENTIFICATION

As per the study, current work focused on study with security and providing a model which include multiple functionality for HER data processing.

The following are the limitation observed which can overcome:

1. The existing algorithm architecture does not support for the Boolean query and thus the quick format of query is not performed which is lacking in current work and can be overcome in proposed research work.

2. The multiple component participation and number of individual algorithms increases the complexity of architecture

which may lead to high computational cost. This can be simplify in proposed architecture.

3. A security with group order 160 bit is proposed which can improve up to 256 bit key and thus an strong key can be generated.

4. High computation cost may lead to fail for common mid-level enterprise which needs an improvement.

5. More attack resilience model can be presented.

4. PROPOSED METHODOLOGY

In order to overcome the existing problem formulation. The following approach over the model is going to include.

1. Encrypted searching mechanism which can also support Boolean search over the encrypted proxy data server.

2. An Fast and efficient encryption technique over the proxy re-encryption and encryption HECC (Hyper elliptic curve cryptography) algorithm can be presented to improve the performance over the existing security approach.

3. Apart from the current attack resilience, some other guessing attack is going to perform to show effectiveness of the system.

4. A Simplified model with less component architecture with high security and searching approach with word relation building approach is going to present.

5. Finally a SAAS platform with mentioned security and searching feature with multi keyword will be presented.

Pseudo Code

Input: CS cloud server, Encrypted data Edi, multi keyword input, Boolean query

Output: Search output, Relevant Data, computation usage, throughput

Steps:

Begin[

Initializing cloud setup();

Processing HECC encrypted data storage;

For each keyword(keyword processing)

{

Finding word relevance;

Boolean breakup();

}

Access indexing from hecc data();

Word relation building;

Boolean search function();

Finding keyword score;

Data matching();

Return;

Attack monitoring();

Data integrity verification();

Return verResult;

Compute utilization();

Computation outcomes;

End];

5. RESULT ANALYSIS

In this section, different observed result which is performed is presented. A statically analysis and graphical analysis using the existing as well as proposed technique is presented.

Experimental Setup

In order to evaluate the complete scenario and execution. The experiment is performed over the net beans using the cloudsim API with the planet lab workload. The workload is processed through the simulation environment with multiple VM and cloudlet data scenario.

The experiment scenarios get performed using the Java programming language over the multiple algorithm and proposed solution using the over utilized scenario of VM and given host.

Computing Parameter

There are mainly three parameter, which is taken for the comparison analysis is taken. Computing parameter such as computation time, computation cost and bandwidth consumption is observed.

Computation Time

Computing time is the time difference which is observed by subtracting final executing time to initial loading time. A time difference between both the times is observed and call as computation time.

Computing Time = Final Execution Time – Initial Time;

Ct=Fet-It;

Computation Cost

Computing cost is the total cost which can be observed by monitoring different usage resources and aspects such as bandwidth, data consumption, resources etc.

Bandwidth consumption

It is the total data consumption per unit of time which is taken by the token and complete access monitoring.

Bandwidth Consumption = Total Data Consumption/ Unit Time;

Bc = Tdc/Ut;

Statistical Analysis

In this section we will explain about the several calculations Performed over different algorithms.

Table 1.1: Comparison Computation Between Existing And Proposed Computation Time At Server End.

ALGORITHM NAME DATA SIZE	EXISTING ECC (SERVER END)	ENHANCE ECC (SERVER END)
5 MB	5654 ms	5654 ms
10 MB	4555 ms	4555 ms
15 MB	11890 ms	11890 ms

In the above table the computation over different files has been shown.

Table 1.2: Comparison Computation Between Existing And Proposed Computation Time At TPA End.

ALGORITHM NAME DATA SIZE	EXISTING ECC (TPA END)	ENHANCE ECC (TPA END)
5 MB	2311 ms	2311 ms
10 MB	1980 ms	1980 ms
15 MB	7123 ms	7123 ms

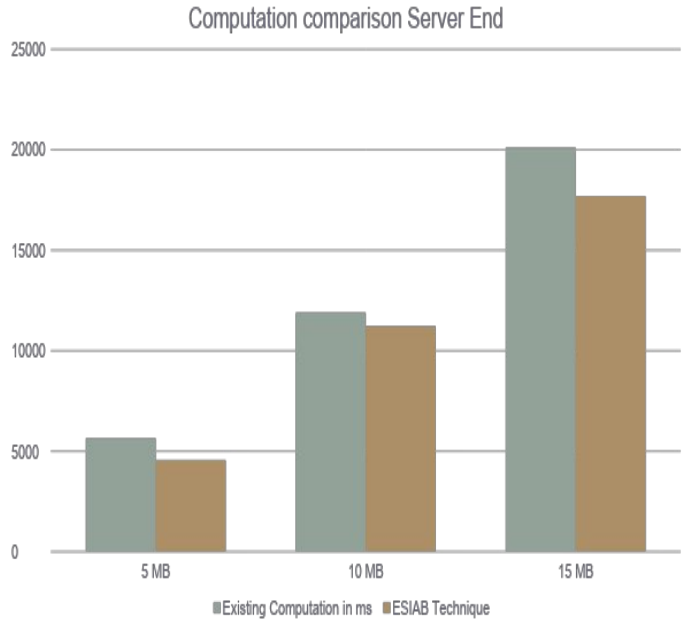

Figure 1.2: Graph Of Computation Time Over Different Files.

The above figure which represents the comparison analysis part in between the Existing ECC based encryption algorithm and the proposed ECC being proposed in our implemented work, the graph shows the efficiency while working at server side.

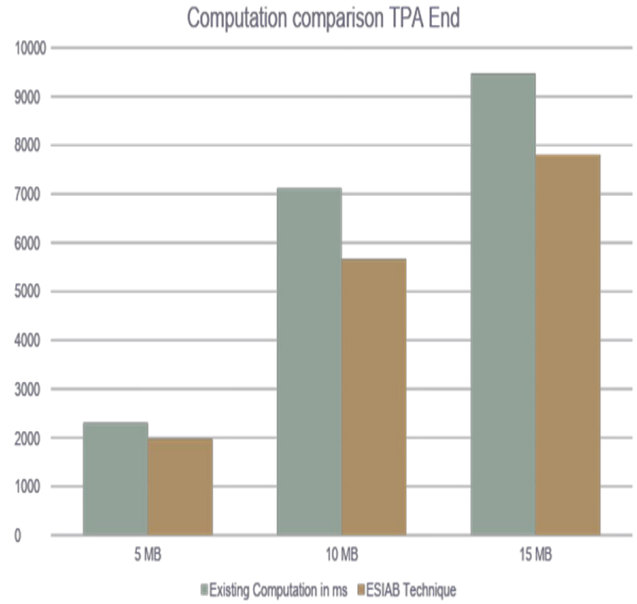

Figure 1.3: Bar Graph Comparison Analysis In Between Implemented Algorithm TPA Side.

The figure above demonstrate the computation time which is being taken while communication performed by the TPA, the operation such as data integrity verification and correctness of data computation data is performed at TPA side , the result comparison given high performance which is shown in above bar graph.

5. CONCLUSION & FUTURE WORK

As per discussed and algorithm performed by us in the area of cloud commutating. The considered work from the traditional algorithm taken as ECC and MAC for the encryption purpose and the key exchange and data distribution among the range of data. The proposed work performed by us is enhancing ECC where the SHA-2 takes part for the key generation and hash tag generation process. Our work also simplify the modules take part in complete process and finally the data is stored in encrypted form and hash tag for the same file id stored, further the integrity verification and proof generation is performed by us. The proposed work is conducted at configured cloud server accessed from remote location using static IP driven. The result we computed using the computation time and key exchange system given by the proposed system outperform better in proposed work. As per analysis the proposed work compute the low time at TPA side as well as server side to process the data store at server side as well as manage and proof generation.

As per discussion the proposed algorithm outperforms best in its field where both the encryption and hashing perform best among. Our further work will be implementing the system and algorithm with multiple authority system and also to perform them in parallel to get our result in heavy traffic cloud environment.

REFERENCES

1 .Soumya Parvatikar, Puja Prakash , Richa Prakash, Pragati Dhawale, S. B. Jadhav Secure Sharing of Personal Health Records utilizing Multi Authority Attribute based Encryption in Cloud Computing, IEEE Transactions On Parallel And Distributed Systems Volume : II, Issue : X, October - 2013.

2. Saipavan Konda,Niranjan Reddy Enhanced Scalable and Secured Sharing of Personal Health Records in Cloud Computing Based on Attribute Based Encryption with Integrity Proof Volume 3, Issue 9, September 2013.

3.Price M, Bellwood P, Kitson N, Davies I, Weber J, Lau F. Conditions conceivably touchy to a Personal Health Record (PHR) intercession, a methodical audit. BMC Med Inform Decis Mak [Internet]. ; 2015:

4. Yoshitaka,S.Chujyou,H.Kato Translation between HL7 v2.5 and CCR message designs (For correspondence among clinic and individual wellbeing record frameworks). Open Systems (ICOS), IEEE Conference on, September 2011.

5 C. J. Wang, X. L. Xu , D. Y. Shi , W. L. Lin Prevalence and pattern of hepatitis C infection disease among blood contributors in Chinese territory: an efficient survey and meta-investigation Published online 2011 Apr 9.

6 P. Van Gorp , M. Comuzzi, An open stage for individual wellbeing record applications with stage level security assurance, Volume 51, August, 2014.

7 M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, Above the Clouds: A Berkeley View of Cloud Computing, Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.

8 Abdulrahman Jabour,JosetteF.Jones, Facilitators and Barriers to Patients Engagements with Personal Health Records: Systematic Review, UAHCI 2013.

9 Cong Wang, Member, IEEE, Sherman S.M. Chow, Qian Wan, Privacy-Preserving Public Auditing for Secure Cloud Storage, IEEE Transactions on Computers (Volume: 62, Issue: 2, Feb. 2013).

10 RachnaArora, AnshuParashar, Maintaining Data Confidentiality and Security over Cloud: An Overview.