International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 07 | July -2017 www.irjet.net p-ISSN: 2395-0072

MULTI-SERVER AUTHENTICATION KEY EXCHANGE APPROACH IN BIGDATA ENVIRONMENT

Miss. Kiran More[1], Prof. Jyoti Raghatwan[2]

[1]Kiran More, PG Student. Dept. of Computer Engg. RMD Sinhgad school of Engineering Warje, Pune
[2]Prof. Jyoti Raghatwan, Dept. of Computer Engg. RMD Sinhgad school of Engineering Warje, Pune

---

Abstract - *The key establishment difficulty is the maximum central issue and we learn the trouble of key organization for secure many to many communications for past several years. The trouble is stimulated by the broadcast of huge level detached file organizations behind similar admission to various storage space tactics. Our chore focal ideas on the current Internet commonplace for such folder systems that is Parallel Network Folder System [pNFS], which generates employment of Kerberos to establish up similar session keys flanked by customers and storing strategy. Our evaluation of the available Kerberos bottommost procedure validates that it has a numeral of borders: (a) a metadata attendant make imaginable key trade over sandwiched amongst the clients and the packing devices has important workload that put a ceiling on the scalability of the procedure; (b) the procedure does not make available frontward confidentiality; (c) the metadata waitron harvests herself all the gathering keys that are cast-off flanked by the clients and packing devices, and this inherently shows the approach to key escrow. In this structure, we advocate an assortment of authentic key trade over measures that are planned to tackle the above problems. We determine that our events are competent of plunging up to coarsely 54 presents of the assignment of the metadata server and concurrently at the bottommost of onward privacy and escrow freeness. All this need only a minute share of superior than before scheming in the gases at the client.*

***Key Words*: Parallel sessions, authenticated key exchange, network file systems, forward secrecy, key escrow.**

1. INTRODUCTION

In similar file organizations, the file numbers are dispersed across multiple storing devices or nodes to allow concurrent access by multiple tasks of a parallel application. That is classically used in huge scale cluster figuring that attentions on high act and reliable get to large datasets. That sophisticated I/O bandwidth is accomplished through coexisting fetching numbers to multiple stowing devices indoors large subtracting clusters, despite the fact data loss is thriving through data imitating using defect forbearing striping procedures.

Few examples of high performance similar file organizations that are in the production use are the IBM Over-all Equivalent Files System. Which are usually required for advanced scientific or data exhaustive applications such as digital animation studios, computational fluid dynamics, and semiconductor manufacturing.

In these milieus, hundreds or thousands of file structure clients bit data and engender very much high summative I/O load on the file coordination supporting petabytes or terabytes scale storage capacities. Liberated of the enlargement of the knot and high-performance computing, the arrival of clouds and the MapReduce program writing model has resulted in file system such as the Hadoop Distributed File System (HDFS).

In this exertion, we examine the issue of the secure many to many communications in the large-scale system file organizations which support parallel fetch to multiple storing devices. That we considering the announcement model anywhere there are a large number of the clients editing many remote and circulated storage diplomacies in parallel.

Particularly, we attempt to attention on how to conversation the key supplies and creation of the equivalent secure sittings between clients and storage campaigns in the parallel Grid File System (pNFS), the up-to-date Internet ethics in efficient and scalable manner. The advance of pNFS is driven by Sun, UMich/CITI, IBM, and EMC. So that it shares many similar countryside and is sociable with many existing commercial network file schemes. Our main goal in this exertion is to design well-organized and secure genuine key exchange protocols that meet specific needs of pNFS. Particularly, we effort to meet the subsequent desirable belongings, which have not.

More specifically, pNFS comprises a collection of three protocols: (i) the pNFS protocol that transfers file metadata, also known as a layout, among the metadata server and a client node; (ii) the storage access protocol which specifies how the client accesses data from the associated storage devices according to the corresponding metadata; and (iii) the control protocol which synchronizes the state among the metadata server and the storage devices.

In this paper, we have proposed Multi-Server Authentication Key Exchange. Section 2 of this paper deals with Literature Survey and Section 3 presents Proposed System. Section 4 concludes this paper.

2. LITERATURE SURVEY

System [1] Tele care Medical Information Systems (TMIS) give a viable approach to increase the medicinal procedure between specialists, attendants and patients. By pleasing to the eye, the security and fortification of TMIS, it is essential while testing to boost the TMIS so that an easygoing and a high-quality can perform corresponding substantiation and session key foundation utilizing a 3-party restorative server while the safe information of the patient can be guaranteed. In proposed framework, an unknown three-party clandestine word legalized key trade (3PAKE) pact for TMIS is utilized. The pact depends on the expert elliptic bend cryptosystem. For security, we apply the pi calculation based proper authorization instrument ProVerif to validate that our 3PAKE contract for TMIS can give secrecy to patient and specialist and additionally accomplishes synchronized verification and session key security. The benefit of planned plan is security and effectiveness that can be used as a part of TMIS. For this J-PAKE based conventions are utilized. The impediment of proposed plan is of it reduced session keys.

In [2] Michel Abdalla, David Pointcheval., "Simple Password Based Encrypted Key Exchange Protocols" Password-based encrypted key exchange are protocols that are future to give combine of clients imparting over a questionable station with a safe assembly key aside when the anonymous key or secret key shared amongst two clients is pinched from a little arrangement of keys. In proposed plot, two straightforward open sesame grounded fixed key trade conventions in assessment of that of Bellovin and Merritt. While one settlement is more reasonable to situations in which the secret key is shared over numerous servers, alternate gives healthier security. Both pacts are as effective, if poorer, as any of the recent twisted key trade conventions in the writing, but then they just require a solitary arbitrary prophet occurrence. The confirmation of safekeeping for both settlements is in the irregular prophet show and in opinion of hardness of the computational Diffe-Hellman issue. Nonetheless, a portion of the methods that we utilize are very not the same as the typical ones and make utilization of new variations of the Diffe-Hellman issue, which are of autonomous intrigue. We additionally give solid relations between the new variations and the standard Diffe-Hellman issue. Preferred standpoint of this plan it is conceivable to discover a few kinds of key. In these dissimilar types of protocols are used like SIGMA, IKE etc.

A. Sai Kumar and P. Subhadra., "User Authentication to Provide Security against Online Guessing Attacks", Passwords are unique of the most common causes of system crashes [3], since the low entropy of passwords makes frameworks helpless against savage compel speculating assaults. Because of innovation passwords can be hacked effectively. Mechanized Turing Tests retain on life a successful, easy to-send way to deal with distinguish robotized malignant login endeavors with sensible cost of bother to clients. Henceforth in this proposed conspire the deficiency of existing and proposed login conventions intended to address large scale online word reference assaults e.g. from a botnet of an enormous number of hubs. In this plan proposed a straightforward plan that reinforces watchword based confirmation conventions and averts online word reference assaults and many-to-many attacks common to 3-pass SPAKA protocols.

Anupam Datta, Ante Derek, John C. Mitchell, and Bogdan Warinschi "Key Exchange Protocols: Security Definition, Proof Method and Applications", System [4] proposed conspire Uses compositional technique for demonstrating cryptographically stable security properties of key trade conventions, in bright of a distinctive rationale that is deciphered over routine keeps running of a convention against a probabilistic polynomial time assailant. Since thinking around an unbounded number of keeps running of a convention includes enlistment like contentions about properties safeguarded by every run, we detail of a secure key trade that, dissimilar to customary key in recognize capacity, is shut under general piece with steps that utilization the key. We exhibition formal authorization rules in assessment of this enjoyment based complaint, and prove that the verification morals are wide-ranging over a computational semantics.

R.S. RamPriya, M.A. Maffina., "A Secured and Authenticated Message Passing Interface for Distributed Clusters", In [5] a public network, at the point when various bunches associated with each other is lengthened turns into a likely danger to security applications running on the groups. To address this issue, a Letter Passing Interface (MPI) is produced to save sanctuary benefits in an unsecured system. The proposed work concentrates on MPI as opposed to different contracts in sunlit of the fact that MPI is a standout amongst the most famous correspondence conventions on appropriated groups. Here AES design is operated for encryption/decoding and introduction polynomial design is consumed for key administration which is then coordinated into Message Transient Interface Trimmer rendition 2 (MPICH2) with typical MPI interface that come to be to be ES-MPICH2. This ESMPICH2 is added MPI that gives refuge and confirmation to conveyed groups which is bound together into cryptographic and mathematical idea. The real longing of ES-MPICH2 is backup a huge collection of cunning and correspondence stages. The proposed agenda depends on both cryptographic and mathematical awareness which prompts to brimming with blunder free memo passing border with improved security.

Feng Hao1 and Peter Ryan2., "J-PAKE: Authenticated Key Exchange without PKI", in [6] password Authenticated Key Argument (PAKE) is unique of the essential subjects in cryptography. It intends to address a pragmatic security issue: how to size up secure correspondence between two gatherings exclusively in sunny of a common secret word without requiring a Public Key Infrastructure (PKI). After over 10 years of broad research in this field, there have been

a few PAKE conventions accessible. The EKE and SPEKE plans are maybe the two most outstanding illustrations. Both systems are however protected. In this rag, we audit these methods in detail and outline different hypothetical and functional shortcomings. Also, we exhibit added PAKE prearrangement called J-PAKE. Our procedure is to bank on upon firm primitives, for case, the Zero-Knowledge Proof (ZKP). As such, the superior part of the past arrangements has withdrawn from exploiting ZKP for the apprehension on proficiency. We display in what manner to successfully coordinate the ZKP into the pact outline and in the interim, accomplish great productivity. Our convention has practically identical computational productivity to the EKE and SPEKE plans with clear advantages on security.

Bruno Blanchet., "Automatically Verified Mechanical Resistant of One-Encryption Key Exchange", System [7] present an automated verification of the secret key based convention One-Encryption Key Exchange (OEKE) utilizing the computationally-solid convention prover CryptoVerif. OEKE is a non-insignificant convention, and accordingly motorizing its verification gives extra certainty that it is right. This contextual investigation was additionally a chance to actualize a few vital expansions of CryptoVerif, valuable for demonstrating numerous different conventions. We have without a doubt stretched out CryptoVerif to bolster the computational Diffie Hellman presumption. We have likewise included support for evidences that depend on Shoup's lemma and extra amusement changes. Specifically, it is presently believable to entrench case refinements physically and to consolidation cases that no longer should be recognized. In the long run, a few upgrades have been involved the calculation of the prospect limits for attacks, giving better cuts. Specifically, we augment over the typical calculation of chances when Shoup's lemma is utilized, which permits us to increase the bound given in a past manual evidence of OEKE, and to authenticate that the enemy can test at most one secret word for each session of the convention. In this tabloid, we introduce these augmentations, with their application to the mark of OEKE. All means of the verification, both programmed and physically guided, are checked by CryptoVerif.

Feng Hao and Peter Ryan., "Password Authenticated Key Exchange by Juggling", System [8] password-Authenticated Key Exchange (PAKE) contemplates how to physique up secure correspondence between two remote gatherings exclusively in light of their mutual watchword, without requiring a Public Key Infrastructure (PKI). Regardless of broad research in the previous decade, this issue stays unsolved. Patent has been one of the chief brakes in sending PAKE arrangements practically speaking. Furthermore, notwithstanding for the licensed plans like EKE and SPEKE, their security is just heuristic; scientists have reported some unpretentious yet stressing security issues. In this rag, we put forward to handle this issue utilizing an approach not quite the same as every past arrangement. Our convention, Password Authenticated Key Exchange by Juggling (JPAKE), accomplishes common validation in two stages: initial, two gatherings send transient open keys to each other; second, they scramble the mutual secret key by juggling people in general keys obviously. The principal utilization of such a juggling method was create in tackling the Dining Cryptographers issue in 2006. Here, we apply it to tackle the PAKE issue, and prove that the convention is zero-learning as it uncovers nothing aside from one-piece data: whether the provided passwords at two sides are the same. With clear points of interest in security, our plan has equivalent proficiency to the EKE and SPEKE protocols.

3. PROPOSED SYSTEM

3.1 Problem statement

To design and implement minimum multiple server file distribution system where we store encrypted data on different servers & the data will be equated & decrypted for authentic user only using MapReduce technique.

3.2 System Architecture

In the proposed work to design and implement a system which can provide parallel processing with key authentication protocol in network file system in Hadoop environment. The system provides Elgamal encryption algorithm for provide the security to distributed data servers. System also prevent SQL injection as well as data collusion attack from external requests. System can automatically manage the load balancing into different data nodes.

Fig 1: Proposed System Architecture

System implementation protocol

pNFS-AKE-I: Our first protocol can be regarded as a modified version of Kerberos which allows the client to generate its own session keys.

pNFS-AKE-II: For address key escrow while achieving forward secrecy concurrently. We incorporate a Diffie-Hellman key agreement technique into Kerberos-like pNFS-

AKE-I. Mainly, the client C and the storage device Si both chooses a secret value and pre-computes a Diffie-Hellman key component and session key is then generated from both the Diffie-Hellman components.

pNFS-AKE-III: Our third protocol aims to achieve full forward secrecy, which is, exposure of a long-term key affects only a current session key, but not all the other past session keys.

3.3 Algorithms

1. Diffie-Hellman Key Exchange Protocol

Diffie–Hellman creates a shared secret which can be used for secret communications while exchanging data on a public network. To implement Diffie-Hellman, the two end users Alice and Bob, while communicating through a channel they equally agree on two positive whole numbers *q* and *g*, such as *q* is a prime number and *g* is a generator of *q*. The generator *g* is a number that, when raised to positive whole-number powers less than *q*, not ever produces the same result for any two such whole numbers. The value of *q* may be large but the value of *g* is typically small.

Once Alice and Bob have agreed on *q* and *g* in private, they choose random positive whole-number *m* and *n*, Next, Alice and Bob compute public keys *A* and *B* based on their personal keys according to the formulas

1) $A = g^m \bmod q$

2) $B = g^n \bmod q$

The two users can share their public keys A and B over a communications medium assumed to be insecure, such as the Internet or a corporate wide area network (WAN). From these public keys, a number x can be generated by either user *based on* their own personal keys.

Alice computes K_1 using the formula,

3) $K_1 = (B)^m \bmod q$

Bob computes K_2 using the formula,

4) $K_2 = (A)\ n \bmod q$

Obviously $K_1 = K_2$, So this will be shared secret key among Alice and Bob.

2. Elgamal Encryption scheme

Key Generation phase

Input: Plain text as text data d.
Output: a,b,p,g all are private keys

Step 1: Initialize the random message from user as d. (it should be any kind of text data).
Step 2: initialize a,b,p,g for private key purpose.
Step 3: generate P as randomly base on bit length of d. so, Ans[] =GetRandomP(d.getbyte).bitlength base on probable prime no.
Step 4: p= Ans[0]
g = Ans[1]
Step 5: Generate a using P
a=RandomA(p)
its calculate like p.bitLength()-1,Random.
Step 6: Calculate b= calculateb(g, a, p);
so, b= g.modPow(a, p);
Step 7: Key generation done

Encryption

Input : Text data d,p,b,g
Output cipher as C1,and C2.

```
initialize BigInteger [] rtn = {null,null};
 message=d.getbytes();
 [] result= ElGamal.encrypt(message, p, b, g);
 [] rtn = {null,null};
k = ElGamal.getRandomk(p);
C1 = g.modPow(k, p);
C2 = m.multiply(b.modPow(k, p)).mod(p);
```

Decryption

Input : input c1 and c2 as cipher a and p as private keys
Output: Plain text d.

```
Step 1:  m = C2.multiply (C1.modPow (a.negate(), p)).mod (p);
Step 2: return m.
```

3.4 Mathematical Module

S1 and s2 get random number r; Calc Prime p;
G=0: p-1
a=S1 get secret number b=S2 get secrete number
Calc = G(ap)
Calc1 = G(bp)
S1 sends calc to s2.
S2 sends calc1 to s1.
S1 = K1 = calc1(ap)
S2 = K2 = calc(bp)
If (k1==k2):true::false

Elgamal Encryption

(p; b; g)
(a)==privatekey
[c1; c2] = enc(data; p; b; g);
Plain = dec(c1; c2; a; p);

4. RESULTS AND DISCUSSION

For the system performance evaluation, calculate the matrices for accuracy. The system is implemented on java 3-tier MVC architecture framework with INTEL 3.0 GHz i5 processor and 8 GB RAM with Hadoop 2.5 in open source

environment. Chart - 1. Shows data encryption as well as decryption performance which works to show that the data it will encrypt in how much time in seconds. Suppose there is a 100kb data is encrypted in 62 sec so the result will display automatically in that time of encryption data from the users.

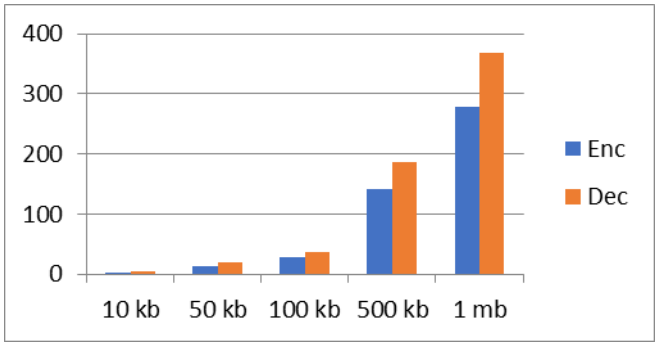

Chart -1: **Server Round Performance**

After the complete implementation of system evaluate with different experiments. For the second experiment system focus on time complexity of cryptography algorithm. The system takes use different time for data encryption as well as data decryption purpose. The below Chart - 2 shows the encryption and decryption time complexity.

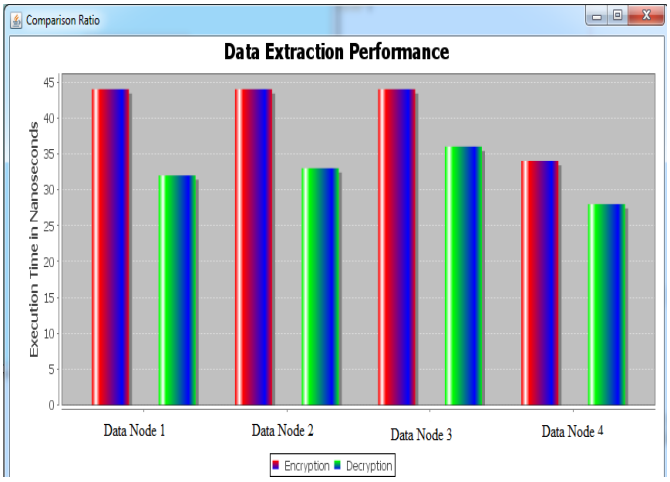

Chart -2: **Data encryption and decryption performance with each data node**

4. CONCLUSIONS

We proposed three real key exchange protocols for equivalent network file system (pNFS). Our etiquettes offer the rewards over the prevailing Kerberos-based pNFS protocol. First, the metadata server implementing our rules has much lower workload than that of the Kerberos-based approach. Second, two our etiquettes provide frontward secrecy: one is somewhat forward secure (with reverence to the many sessions within a time period), whereas the other is fully forward safe as houses (with reverence to a session). Third, we have designed a protocol which not only provides forward secrecy, but is also escrow-free.

5. FUTURE WORK

The suggested work carries on the line of enquiry on the two-server standard in, extend the model by imposing diverse levels of expectation upon the two servers, and adopt a very different method at the technical level in the procedure design. As a result, we suggest a practical two-server PIN authentication and key argument system that is sheltered against disconnected dictionary doses by servers when they are controlled by adversaries. The future scheme is a PIN-only arrangement in the logic that it requires no civic key cryptosystem and, no PKI. For the system future enhancement, we can focus on dynamic slot configuration approach using MapReduce framework for similar network file system.

ACKNOWLEDGEMENT

It is my privilege to acknowledge with deep sense of gratitude to my guide Prof. Jyoti Raghatwan for her kind cooperation, valuable suggestions and capable guidance and timely help given to me in completion of my paper. I express my gratitude to Prof. Vina M. Lomte, Head of Department, RMDSSOE (Computer Dept.) for her constant encouragement, suggestions, help and cooperation.

REFERENCES

[1] Hoon Wei Lim and Guomin Yang., "Authenticated Key Exchange Protocols for Parallel Network File Systems",IEEE Trans. On Parallel And Distributed Systems, Vol. 27, No. 1, January 2016, pp.1045-9219.

[2] Qi Xie1, Bin Hu1, Na Dong1, Duncan S. Wong2 ., "Anonymous Three-Party Password-Authenticated Key Exchange Scheme for Telecare Medical Information Systems", in june 2014.

[3] Fabrice Benhamouda and David Pointcheval,"Verifier-Based Password-Authenticated Key Exchange: New Models and Constructions", in October 2014.

[4] *A. Sai Kumar and **P. Subhadra., "User Authentication to Provide Security against Online Guessing Attacks", Feb 2013.

[5] Anupam Datta1, Ante Derek1, John C. Mitchell1, and Bogdan Warinschi2., "Key Exchange Protocols: Security Definition, Proof Method and Applications", in 2013.

[6] R.S.RamPriya, M.A.Maffina., "A Secured and Authenticated Message Passing Interface for Distributed Clusters", IEEE ,2015.

[7] Feng Hao1 and Peter Ryan2., "J-PAKE: Authenticated Key Exchange Without PKI", in 2010.

[8] Bruno Blanchet., "Automatically Verified Mechanized Proof of One-Encryption Key Exchange", in 2012.

[9] Feng Hao and Peter Ryan., "Password Authenticated Key Exchange by Juggling", Springer, pp. 159-171,2011.

[10] Dr. Durgesh Kumar, Neha Koria, Nikhil Kapoor, Ravish Bahety, "A Secure Multi-Party Computation Protocol for Malicious Computation Prevention for Preserving Privacy During Data Mining", International Journal of Computer Science and Information Security,Vol. 3., 2009.

[11] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proceedings of the Network and Distributed System Security Symposium, 2012.

BIOGRAPHIES

Miss. Kiran B More BE (Computer) Completed, ME Second year Student of R.M. Dhariwal Sinhgad School of Engineering, Pune.