Key Exchange Protocols for Parallel Network File Systems Using Optimized Cryptography

Inam Abdullah Lafta1, Ruaa Ali Khamees2, Rana Alauldeen Abdulrahman3
1ICT Department, Institute of Technology, Middle Technical University, Baghdad, Iraq.
2Department of Civil Technologies, Institute of Technology, Middle Technical University, Baghdad, Iraq.
Email: inam.abdullah96@mtu.edu.iq, dr.ruaakhamees@mtu.edu.iq, rana.ala@mtu.edu.iq

Abstract: The utilization of parallel file system is expanding quickly nowadays; security moves toward becoming are significant worry about inside this work is to structure capable and secure affirmed key trade conventions that meet explicit necessities of pNFS. The current techniques neglected to achieve alluring properties, for instance, scalabiliy, viability, escrow free and forward mystery. A large portion of existing techniques either has not been alluringly practiced or are not reachable by the current Kerberos-based arrangement. These issues overwhelmed by a late technique which is utilizing an assortment of authenticated key trade conventions that are intended to address the above issues. This technique utilized AES calculation for security. In this undertaking, It is giving that a new AES calculation objective of accomplishing speed and security. This new AES is called as IAES (improved AES). The proposed security technique will accomplish better execution as far as speed, security, and correspondence overhead when contrasted with existing strategies.

Keywords: AES, Parallel NFS, Protocols.

1. Introduction
In a parallel documenting system, report learning is scattered over various limit devices or center points to permit synchronous access taken by different assignments of a parallel application. This can be commonly used in colossal scale group handling which spotlights on preferred execution and solid access over enormous datasets. That is, higher I/O information measure is master through synchronous access to different limit contraptions at interims enormous figure clusters; while information setback is verified through learning reflecting abuse deficiency tolerant checking algorithms.

Key-trade protocols region unit systems by those 2 parties that impart over partner antagonistic controlled system will create a standard mystery key. Key protocols are basic for empowering the work of shared-key cryptography to shield transmitted information over shaky networks. They are a focal piece for structure secure interchanges, and region unit among the preeminent commonly utilized cryptographical protocols (contemporary precedents grasp SSL, IPSec, SSH, among others) [1].

System appended plates financially offered nowadays do not give any help for security: they respect any solicitation got. Accordingly, verifying a nicotinamide adenine dinucleotide order system today needs the nicotinamide adenine dinucleotide to arrange and each one snared machines and plates to be physically verified. In apply, this powers the work of a different LAN for capacity (as a rule alluded to as a fenced in area System, or SAN) and averts customers arranged outside a machine space or underneath end-client the executives from straightforwardly getting to the NADs [2]. Tragically, this proposes nicotinamide adenine dinucleotide file systems can not convey high information measure to work area machines, avoiding numerous accommodating applications (e.g., action training...
recordings to PCs and work area learning to mine) from exploiting nicotinamide adenine dinucleotide innovation.

The Google documenting system (GFS) is organized and maintained to satisfy the quickly creating solicitations of Google’s information dealing with needs. GFS shares a couple of practically identical destinations as past appropriated record structures, for example, execution, scalability, duty, and handiness. Regardless, its structure has been driven by key perceptions of our application remaining weights and innovative condition, each present and anticipated, that copy a checked takeoff from some before record system style doubts. It has been reevaluated out of date decisions and researched significantly absolutely phenomenal concentrations inside the arranged house [3].

In the first place, part disillusionments are the standard instead of the exemption. The documenting structure involves enormous measures of or potentially countless limit machines arranged from modest trade stock segments and is gotten to by a proportional variety of client machines. The number and nature of the parts about certification that some don not appear to be deliberate at some random time and a couple won't get over their present disappointments. It not seen the issues brought about by application bugs, operating system bugs, human errors, and in this manner the disappointments of circles, memory, connectors, systems administration, and power give. Along these lines, steady perception, mistake recognizable proof, adjustment to interior disappointment, and customized recovery should be essential to the structure.

Section II present a brief review of related works. In section III, the design of the proposed methodology presented. In section IV, the results are presented. In section V, conclusion and future work disclosed.

2. Literature Survey

This section presents the review of different methods presented for taxonomy construction of keyword from the dataset. In [1] the author has examined the trouble of key foundation for secure many-to-different trades. The inconvenience is influenced by the duplication of expansive scale dispersed record structures giving parallel access beyond what many would consider possible devices. That work dependent on the present Web the standard for such record structures, i.e., parallel System File System (pNFS), which makes use of Kerberos to make parallel session keys among clients and cutoff contraptions. Their examination of the current Kerberos-based custom exhibits that it has particular constraints: (I) a metadata server engaging key trade between the customers and the farthest point devices has tremendous phenomenal weight that restrains the adaptability of the convention; (ii) the convention doesn't give the forward mystery; (iii) the metadata server makes it entire the session keys that are utilized among the customers and limit contraptions, and this unquestionably prompts key escrow. In this given paper, they propose a system of demanded key trade protocols that are relied on to address the previously mentioned challenges.

In [2] Author exhibited the presentation in 2011, the very particular isogeny Diffie-Hellman (SIDH) key trade convention has engineered itself as a promising contender for post-quantum cryptography. One detectable bit of the SIDH custom is that it necessities astoundingly short key sizes. In any case, the torpidity related to SIDH is higher than the ones revealed for other post-quantum cryptosystem recommendations. Which intends to empower the SIDH runtime execution, they accessible in given work a couple of algorithmic sorts of advancement focusing on both elliptic-bend and field number-crunching assignments. They, in addition, present a refreshed examination of the point significantly increasing formula and talk about two or three algorithmic and usage systems that incite quicker field number-crunching figurings.

In [3] Author showed the Authenticated key trade protocols anticipate an essential occupation in tying down exchanges and are extensively sent for used inside various kind of genuine system applications. Diffie-Hellman key trade convention has been generally utilized for stirring up a riddle that enters in two-party trades without utilizing any outcast key association segment. In any case, the Diffie-Hellman key trade convention does not declare the clients in the correspondence and is unprotected against man-in-the-center assault when nature is remote. They appear, an arrangement of Diffie-Hellman key trade convention subject to string examination has been agreeable that locations with the security vulnerabilities found in the unessential Diffie-Hellman Custom.
In [4] the author proposed the security issues accept an essential occupation in current correspondence universes. By methods for questioned networks, exchanged messages ought to be encoded by a session key for security necessities. Session keys are gotten a kick out of the opportunity to be made by discourse gatherings, and how to support the other dialog gathering is a fundamental issue that should have been settled. In three-party encoded key trade (3PEKE) protocols, special sort of wandering authenticated protocols, a trusted outsider is melded to have two correspondence gatherings can bolster each other and orchestrate one session key. In 2008, Yoon and Yoo proposed a three-party scrambled key trade convention and showed their convention gives an increasingly secure way to deal with oversee exchanging messages. Grievously, they find that their convention encounters an intangible one-line puzzle state evaluating assaults. In this unique duplicate, the essential surveys the basic related works and show to mount assaults on Yoon and Yoo's 3PEKE convention.

In [4] the author proposed the quick improvement of electronic innovation; diverse sort of the portable is made to make human life the all the more satisfying. With the cell phones are valuable; people can do some standard trades on Web or remote at whatever point and any place. The best technique to make the discussion security in such contraptions is none inconsequential thing than one may at first look since some current authenticated key trade cannot genuine to be connected with telephone As a result of beyond what many would consider possible and point of confinement is obliged, in this paper, maker proposes a character based supported key trade convention without using bilinear pairings or Weil mixing. Differentiated and past ID-based protocols, our protocols can confine computational over-weight and extra room without extra message trade time.

In [5] Author displayed Secret word Authenticated Key Trade (PAKE) protocols draw in two fragments to make a critical essential session key and embrace each other dependent on a pre-shared human essential riddle key. In 2006, Strangio proposed the DH-BRAKE convention and showed that the made reference to the convention is actually solid inverse two or three assaults. Given paper, it was demonstrated that the DH-BRAKE convention is weak against riddle word exchange off emulate assault and it was assuredly not gifted in light of the number of running advances and its computational burden. To beat these shortcomings, an improved PAKE convention is proposed which gives a few security properties. Moreover, it was demonstrated that their proposed course of action is more sefficient1 (Secure and Incredible) in the examination with DH-BRAKE convention.

In [7] author showed that a key trade convention is an essential thing in the field of information and system security and is used to trade an average puzzle key among various gatherings. Particular key trade protocols exist in the plan and by far most of them rely on the Diffie-Hellman (DH) issue. In any case, these DH type protocols cannot maintain a strategic distance from the bleeding edge processing headways like quantum registering, network figuring, etc. Thusly, an even more unbelievable non-DH type key trade convention is irreplaceable which could limit the quantum and exponential assaults. In the year 2013, Lei and Liao, along these lines proposed transversely over area based key trade convention. Their convention was identified with the NTRU-Scramble and NTRU-SIGN as was alluded as NTRU-KE.

In [8] author displayed that the key trade convention using passwords achieved inconceivable thought on account of its ease and adequacy. On the other hand, the convention ought to restrict a wide scope of mystery word theorizing assaults, since the riddle clarification is of low entropy. Beginning late Chang and Chang proposed a novel three gathering primary key trade convention. They guaranteed the convention was secure, important and sensible. Repealing their cases Yoon and Yoo showed an indistinct online mystery word guessing assault on the above convention. In the present paper, an updated convention has been proposed to butcher dubious online riddle shows guessing assault proposed by Yoon and Yoo. What's more, the proposed updated convention could accomplish better execution limit by requiring just four message transmission rounds and the execution is poor down on an all-out game-plan of investigations.

In [1] the author proposed that the Secret word authenticated key trade (PAKE) is the spot a client and a server, who offers a mystery expression, confirm each other and in the meantime develop a cryptographic key by the trade of messages. In this setting, most of the passwords central to attest customers are verified in a solitary server. On the off chance that the server is endangered, due to, for example, hacking or much insider assault, passwords set away in the server are absolute uncovered. In
the given paper, they accept a situation where two servers take an interest to endorse a customer and if one server is risked, the aggressor still cannot affirm to be the customer with the information from the traded off the server. Most recent reactions for two-server PAKE are either symmetric as in two partner servers correspondingly add to the approval or lopsided in the sense one server explains the customer with the assistance of another server.

In [9] the author introduced that the NEWHOPE and NEWHOPE-Direct these are the two starting late proposed post-quantum key trade protocols reliant on the hardness of the Ring-LWE inconvenience. In light of their high-security edges and execution, there have starting late been talks and propositions for intertwining them into Web benchmarks, like TLS, and mystery masterminds protocols, like Tor. In this work, they present steady time and consistent propelled executions of NEWHOPE and NEWHOPE-Central for ARMv8-A 64-bit processors which target quick applications. This structure is recognized in a creation number of cutting-edge cell and tablet processors and highlights earth-shattering 128-piece SIMD assignments given by the NEON Motor.

3. Methodology

3.1 Problem Definition
In the present parallel file systems, dispersion of record information is done over different limit devices or center points all together grant synchronous access by various errands of a parallel application. This is routinely utilized in expansive scale gathering dealing with those based on high and solid access to huge datasets. In this way, security is the principal worry to accomplish in such file systems. There are numerous security techniques displayed on parallel file systems yet neglected to accomplish every single alluring property of security. For any security strategy, proficiency is chosen by properties like scalability, forward mystery and escrow free. The ongoing techniques are not agreeably accomplishing this property. Thusly this turns into the provoking errand for analysts to display a proficient and adaptable key trade convention for security in pNFS systems. To address these confinements, as of late one new strategy presented for effective and secure key trade convention utilizing AES and SHA-1 Algorithms for pNFS systems. Anyway, in future AES might be a week and slower to ensure pNFS systems, subsequently, there is still an extension to do improvement in security and speed.

3.2. Proposed Work:
Security moves toward becoming are really worrying about in this work it is to structure skillful and secure authenticated key trade protocols that meet specific precondition of pNFS. The current methodologies neglected to achieve the alluring properties, for instance, scalability, effectiveness, escrow free and forward puzzle. By far most of the existing techniques either has not been alluringly cultivated or is not reachable by the current Kerberos-based arrangement. These issues overwhelmed by a late technique that is utilizing an assortment of authenticated key trade protocols that are intended to address the above issues. This strategy utilized AES calculation for security. In this task, a new AES calculation objective of accomplishing speed and security should be giving. This new AES is called as IAES (improved AES).

The proposed security strategy will accomplish better execution as far as speed, security, and correspondence overhead when contrasted with existing strategies.
3.2 Encryption Overview:

Encryption is one of the most utilized techniques for cryptography messages or data in such the least complex way that exclusively endorsed gatherings will peruse it. Secret composing does not of itself hinder capture attempt, anyway, denies the message substance to the contender. In partner secret composition subject, the alleged discourse information or message talked as plaintext, is encoded misuse relate riddle making rule, making figure content which will solely be scrutinized at whatever point decoded. For specific reasons, relate secret forming subject here and their usages a pseudo-arbitrary riddle creating key delivered by partner rule. It is fundamentally feasible to change the message while not having the key, in any case, for a well-structured secret composition subject, monster method assets and capacity are required. An affirmed beneficiary will basically revamp the message with the key given by the conceiver to beneficiaries, any way to not unauthorized interceptors. Half and half AES encryption algorithms are utilized to apply greater security to the information which it should be sharing.

Algorithm 1: Block Based Hybrid Encryption Algorithm

Step 1: Receive Input file
Step 2: Apply introductory change by partitioning info file similarly separated into two squares of equivalent size
M0 = n/2;
N0 = n/2;
[Note: M for left side and N for right side]
Step 3: Apply second dimension change utilizing beneath conditions, isolate further every square in two equivalent amounts.
MM0 = M0/2;
MN0 = M0/2;
NM0 = N0/2;
NN0 = N0/2;
Step 4: Apply DES utilizing Key on every one of the four components of file independently.
Key = 128 bits
MM1 = DES (MM0, key);
MN1 = DES (MN0, key);
NM1 = DES (NM0, key);
NN1 = DES (NN0, key);
**Step 5:** Marge hinders at Second Dimension after DES
\[ fM0 = MM1 + MN1; \]
\[ fN0 = NM1 + NN1; \]

**Step 6:** XOR first level file blocks
\[ \text{Out} = (fM0 \text{ XOR } fN0); \]

**Step 7:** Apply AES on output of XOR
\[ N1 = \text{AES (Out, key)}; \]

**Step 8:** \[ M1 = fN0 \]

**Step 9:** Create Encrypted File
\[ \text{Encrypted} = N1 + M1 \]

**Algorithm 2: Block Based Hybrid Decryption (At Receiver)**
After crossover encryption, at the got side, underneath steps led to recuperate the unique file

**Step 1:** Getting info scrambled file.

**Step 2:** Apply introductory change by partitioning information scrambled file into two equivalent squares of the same size
\[ M0 = n/2; \]
\[ N0 = n/2; \]

[Note: M for left side and N for right side]

**Step 3:** Apply AES on N0
\[ \text{Key} = 128 \text{bits} \]
\[ N1 = \text{AES (N0, key)}; \]

**Step 4:** XOR N1 with M0
\[ \text{OutN} = (N1 \text{ XOR } M0); \]

**Step 5:** Produce left yield utilizing N0
\[ \text{OutM} = N0; \]

**Step 6:** First Dimension Parcel
\[ \text{MM0} = \text{OutM}/2; \]
\[ \text{MN0} = \text{OutM}/2; \]
\[ \text{NN0} = \text{OutN}/2; \]
\[ \text{NM0} = \text{OutN}/2; \]

**Step 7:** Apply DES with Key on each of the four sections separately
\[ \text{Key size utilized here for DES is 128 bits} \]
\[ \text{MM1} = \text{DES (MM0, key)}; \]
\[ \text{MN1} = \text{DES (MN0, key)}; \]
\[ \text{NM1} = \text{DES (NM0, key)}; \]
\[ \text{NN1} = \text{DES (NN0, key)}; \]

**Step 8:** Consolidate Decrypted file squares
\[ \text{M0} = (\text{MM1+MN1}); \]
\[ \text{N0} = (\text{NM1+NN1}); \]

**Step 9:** Create a Decrypted file
\[ \text{Decrypted} = \text{M0+N0}; \]

4. **Results of Practical Work**
The exploratory examination and execution assessment are performed utilizing the KDD inquire about the dataset. A similar investigation is introduced in the middle of discovery time, exactness, accuracy, and review rates.
Figure 2. Time comparison.

The relative examination is displayed between the ongoing technique pNFS announced in [10] and the proposed strategy. Accuracy is computed according to performance of system to construct taxonomy.

Figure 3. Accuracy Comparison

Figure 4. Precision Comparison
In this section, detailed results for existing and proposed method are separately presented and discussed. This helps to understand the Time, Accuracy, Precision and Recall comparison of existing and proposed method. The new AES algorithm helps to improve the speed and accuracy performance as compared to recent method. This new AES is called as IAES (Improved AES). The proposed security method will achieve better performance in terms of speed, security and communication overhead as compared to existing AES methods.

5. Conclusion and Future Work
Three key exchange protocols for parallel network file system (pNFS) are proposed. To maintain security of data, Advanced AES Encryption which is also called as Hybrid AES should be used. Our protocols give three appealing blessings over the present Kerberos-based pNFS protocol. To begin with, the information server execution our protocol has a considerable measure of brings down work than that of the Kerberos-based technology. Second, our protocols offer forward mystery: one is to some degree forward anchoring; however, the reverse is totally forward secured (with importance a session). Third, organizing the protocol that not only provides forward mystery, as well as it also is provides escrow-free.

References
[1] Xun Yi, San Ling, Huaxiong Wang, 2012 Efficient Two-Server Password-Only Authenticated Key Exchange, DOI: 10.1109/TPDS.2012.282.
[2] Yun Wei, Fushan Wei, Chuangui Ma, 2014 Certificateless non-interactive key exchange protocol without pairings, Published in 2014 11th International Conference on Security and Cryptography (SECRYPT).
[3] Qingfeng Cheng, Guanguo Han, Chuangui Ma, 2009 Analysis of Two Authenticated Key Exchange Protocols, DOI: 10.1109/MINES.2009.42.
[4] Li Xiaoyong, Zhang Hui, 2010 Identity-based authenticated key exchange protocols, DOI: 10.1109/ICEIT.2010.5608417.
[5] Maryam Saeed, Ali Mackvandi, Mansour Naddafiu, Hamid reza Karimnejad, An enhanced password authenticated key
[6] Daya Sagar Gupta, G. P. Biswas, Roushan Nandan, 2018 Security weakness of a lattice-based key exchange protocol, DOI: 10.1109/RAIT.2018.8389018.
[7] Hsu-Hung Chiang, Ching-Chung Liu, Ying-Ming Chen, Ya-Fen Chang, 2009 Security of Indirect-Authenticated Key Exchange Protocol, DOI: 10.1109/IH-MSP.2009.136.
[8] R. Padmavathy, Tallapally Shirisha, M. Rajkumar, Jayadev Gyani, 2010 Improved Analysis on Chang and Chang Password Key Exchange Protocol, DOI: 10.1109/ACT.2009.197.
[9] Silvan Streit, Fabrizio De Santis, 2017 Post-Quantum Key Exchange on ARMv8-A: A New Hope for NEON Made Simple, DOI: 10.1109/TC.2017.2773524.

[10] Hoon Wei Lim, Guomin Yang, 2015 Authenticated Key Exchange Protocols for Parallel Network File Systems, DOI: 10.1109/TPDS.2015.2388447.