International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

DUAL-SERVER PUBLIC-KEY ENCRYPTION WITH KEYWORD SEARCH FOR SECURE CLOUD STORAGE

PROF.GOURI PATIL, SRISH, SHAIKH MOHAMMAD SHOAIB, SHIVPRASAD M YELMADGI

ABSTRACT

Searchable encryption is of increasing interest for protecting the data privacy in secure searchable cloud storage. In this paper, we investigate the security of a wellknown cryptographic primitive, namely, public key encryption with keyword search (PEKS) which is very useful in many applications of cloud storage. Unfortunately, it has been shown that the traditional PEKS framework suffers from an inherent insecurity called inside keyword guessing attack (KGA) launched by the malicious server. To address this security vulnerability, we propose a new PEKS framework named dual-server PEKS (DS-PEKS). As another main contribution, we define a new variant of the smooth projective hash functions (SPHFs) referred to as linear and homomorphic SPHF (LH-SPHF). We then show a generic construction of secure DS-PEKS from LH-SPHF. To illustrate the feasibility of our new framework, we provide an efficient instantiation of the general framework from a Decision Diffie–Hellman-based LH-SPHF and show that it can achieve the strong security against inside the KGA

Keywords: Encrytpion, Cloud Storage, Dual-Server

1. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers. Cloud Computing comprises three different service models, namely Infrastructure-as-aService (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. The model is shown in figure below. If a cloud user accesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If she accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider

2. SYSTEM ANALYSIS

Like any other system development model, system analysis is the first stage of development in the event of Object Modeling as well. At this stage, the developer communicates with the system user to determine the user's needs and analyzes the system to understand performance.

* *Corresponding author.*
E-mail address: srish18723@gmail.com

Based on this program study, the analyst prepares the program model you want. This model is based on what the program needs to do. Currently the startup details are not taken care of. Only a system model is based on the idea that the system is made up of a set of components. The essentials of the program are emphasized.

2.1 EXISTING SYSTEM

In the PEKS system, using the recipient public key, the sender pastes encrypted keywords (called PEKS cipher scripts) with encrypted details. The recipient then sends the keyword trap to be searched on the server to search for data. Given the trapdoor and PEKS cipher text, the server can check that the keyword under PEKS cipher txt corresponds to the one selected by the recipient. If so, the server sends the same encrypted data to the recipient.

Back et al. proposed a new PEKS system without the need for a secure route, called the PEKS faultless (SCF-PEKS).

2.2PROPOSED SYSTEM

Contributions for this paper are fourfold. We are validating the PEKS framework called Dual-Server Public Key Encryption with Keyword Search (DS-PEKS) to address PEKS security risks.
A new variant of the Smooth Projective Hash Function (SPHF), called Linear and homomorphic SPHF, was introduced with the standard design of the DS-PEKS.

2.3 ADVANTAGES OF PROPOSED SYSTEM:

Contributions for this paper are fourfold. We validate a PEKS framework called Dual-Server Public Key Encryption with Keyword Search (DS-PEKS) to address PEKS security risks.
A new variant of the Smooth Projective Hash Function (SPHF), called Linear and homomorphic SPHF, was introduced with the standard DS-PEKS design.

3. IMPLEMENTATION

3.1 MODULES DESCRIPTION:

3.1.1 Setting up Network Model

The program consists of four stages, structural installation, customer joining, previous package handling and batch testing. With our basic protocol, in the opening phase of the building, the property owner makes his or her opening and secret keys, after which an open parameter is installed on top of all pre-organization hub systems. During customer integration, the client receives a side-by-side distribution benefit to the program owner. In the pile preparation phase, in the package verification section, the hub checks each pile found. In the event that the result is valid, you update the details as shown in the received package. In this article, each section is presented in detail.

3.1.2 System Initialization Phase

At this stage, the system proprietor performs the corresponding steps to determine the private key and a few open parameters. then it selects the secret key and the key number of the key. From that point forward, the open parameter is loaded first into all system hacks.

3.1.3 User Joining Phase

This category should be done at any time by the client using the U-ID character, which plans to receive the benefit category. Client selects a private key and processes the open key. The client then sends the UID to the owner of the system, in which Prij demonstrates a client breakup benefit. After receiving this message, the system owner generates an announcement.

3.1.4 Packet Pre-Processing Phase

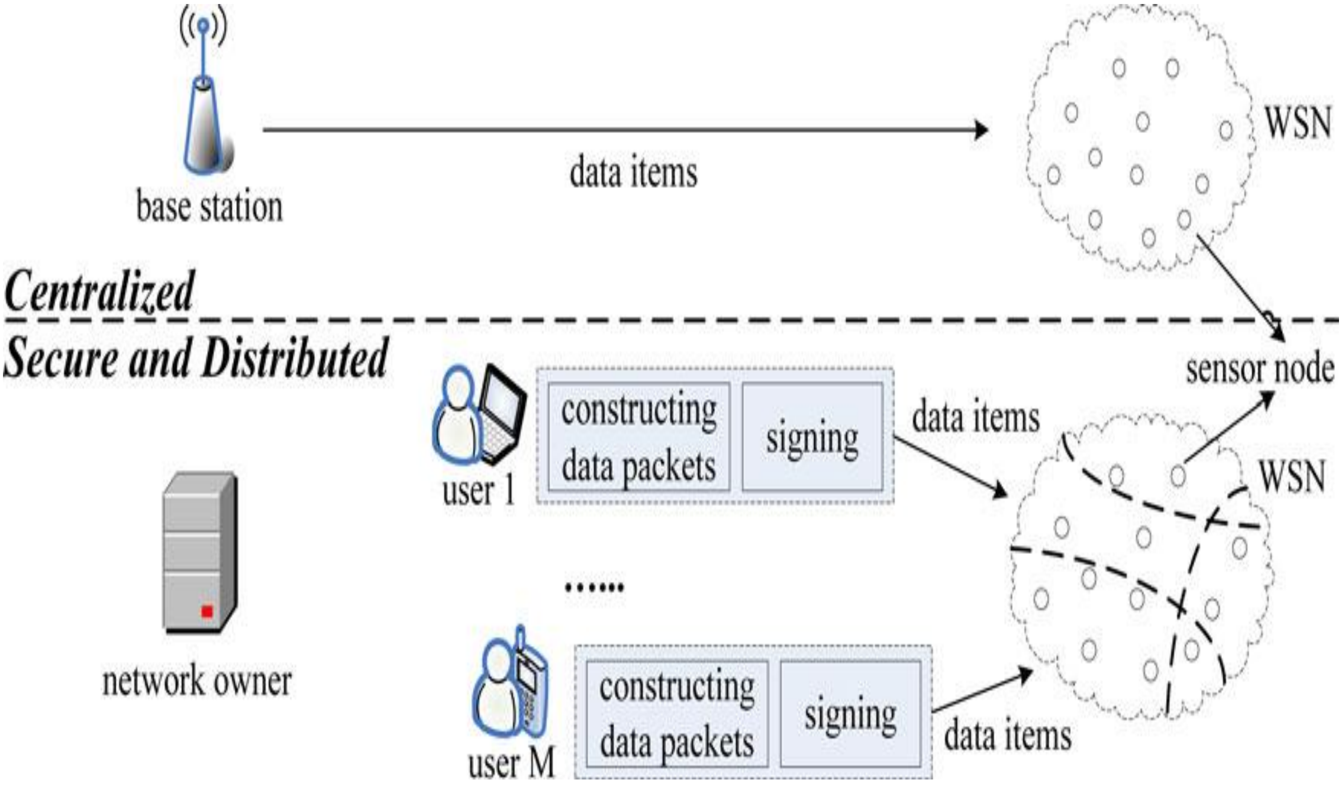
Expect so as to a client, enter the WS-N plus needs to scatter n information things used for the development of the parcels of the individual information, we have two strategies

3.1.5 Packet Verification Phase

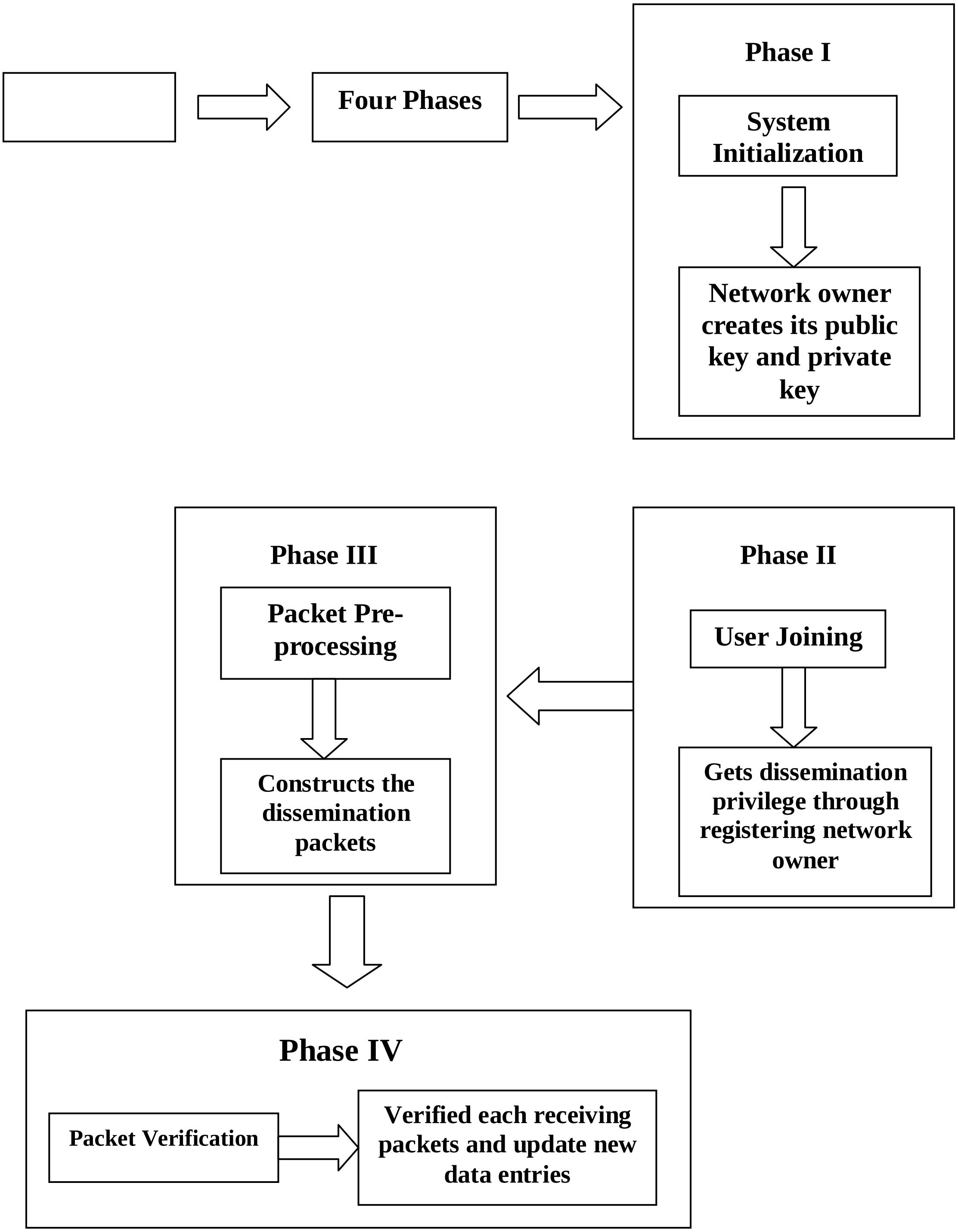
Next exactly at any time the sensor hub, status, find the package and as a client or one of his bold neighbors, first, looks at the main location of the package. If you look at the two strategies, the information hash strategy brings a little bit of visual visibility.

4. SYSTEM DESIGNS

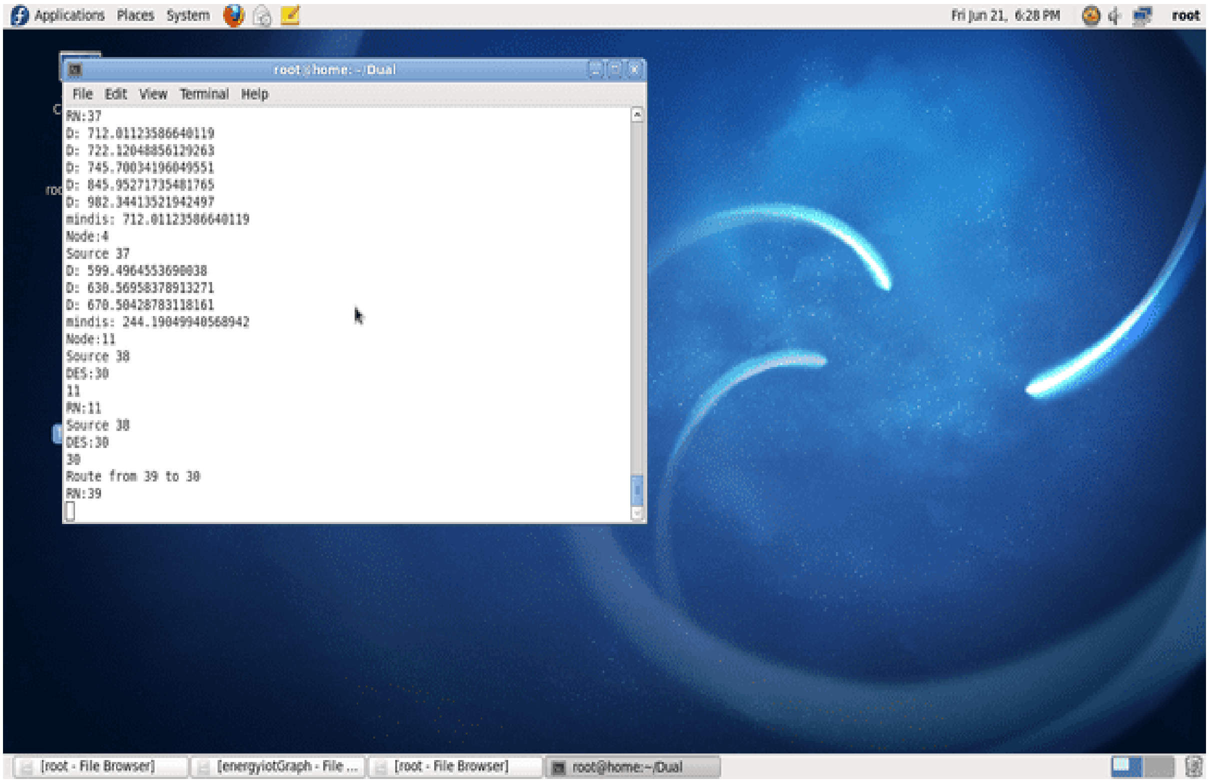
4.1 SYSTEM ARCHITECTURE:



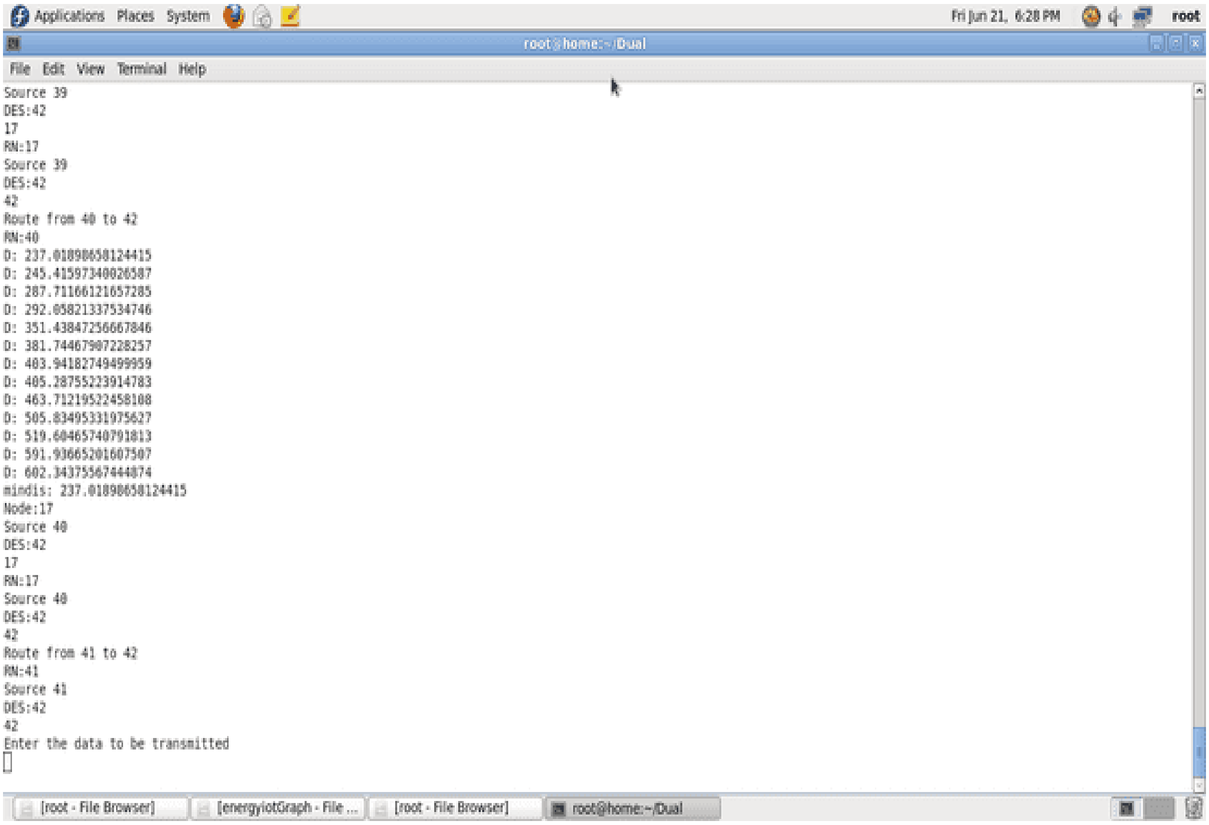
4.2 BLOCK DIAGRAM:


Four Phases
Phase I
System Initialization
Network owner creates its public key and private key
Phase III
Packet Pre-processing
Constructs the dissemination packets
Phase II
User Joining
Gets dissemination privilege through registering network owner
Phase IV
Packet Verification
Verified each receiving packets and update new data entries

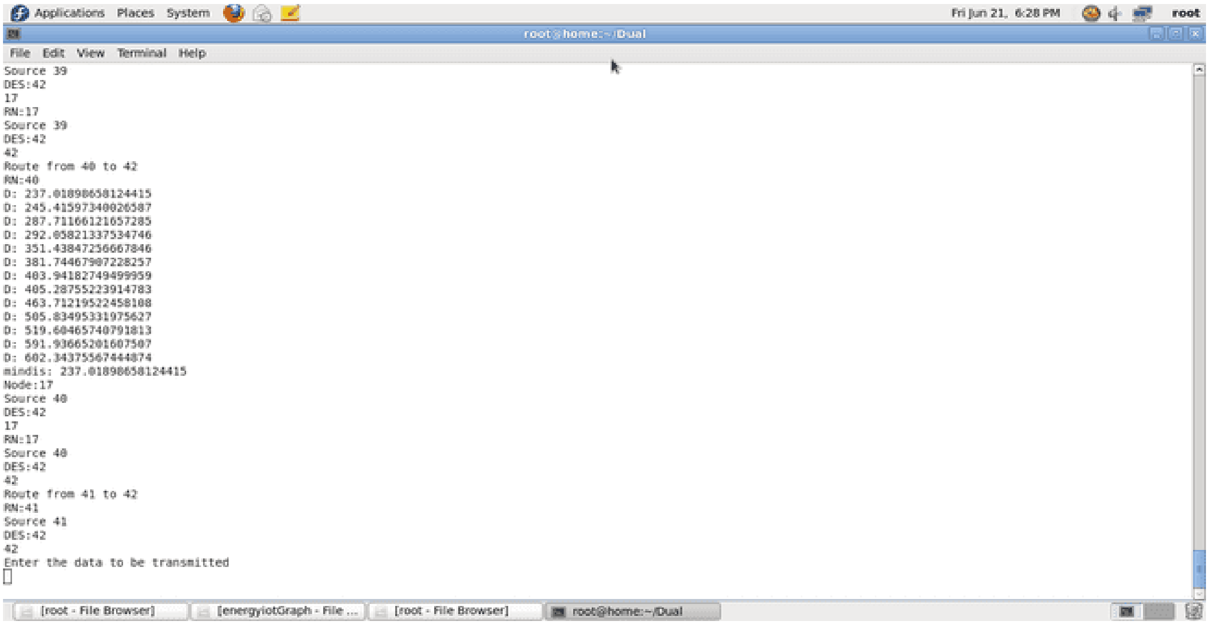
4.3 OUTPUT SCREEN



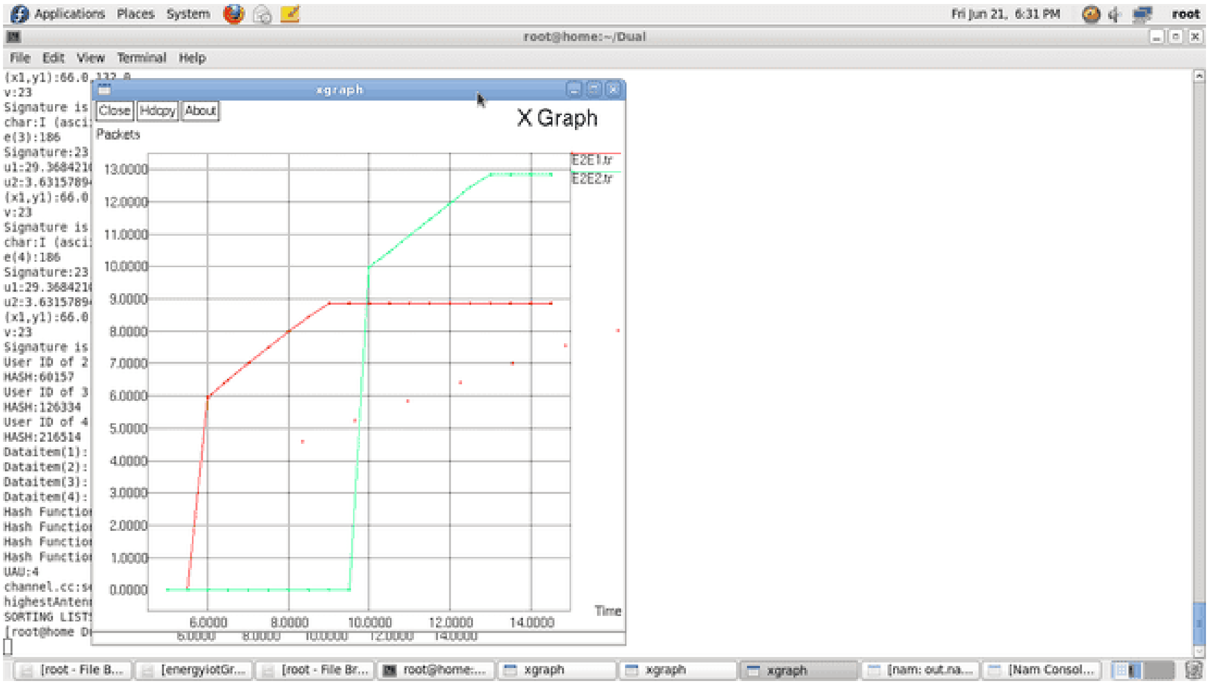
```
RN:37
D: 712.01123586640119
D: 722.12048856129263
D: 745.70034196049551
D: 845.95271735481765
D: 982.34413521942497
mindis: 712.01123586640119
Node:4
Source 37
D: 599.4964553690038
D: 630.56958378913271
D: 670.50428783118161
mindis: 244.19049940568942
Node:11
Source 38
DES:30
11
RN:11
Source 38
DES:30
30
Route from 39 to 30
RN:39
```



```
Source 39
DES:42
17
RN:17
Source 39
DES:42
42
Route from 40 to 42
RN:40
D: 237.01898658124415
D: 245.41597340026587
D: 287.71166121657285
D: 292.05821337534746
D: 351.43847256667846
D: 381.74467907228257
D: 403.94182749499959
D: 405.28755223914783
D: 463.71219522458108
D: 505.83495331975627
D: 519.60465740791813
D: 591.93665201607507
D: 602.34375567444874
mindis: 237.01898658124415
Node:17
Source 40
DES:42
17
RN:17
Source 40
DES:42
42
Route from 41 to 42
RN:41
Source 41
DES:42
42
Enter the data to be transmitted
```



```
Source 39
DES:42
17
RN:17
Source 39
DES:42
42
Route from 40 to 42
RN:40
D: 237.01898658124415
D: 245.41597340026587
D: 287.71166121657285
D: 292.05821337534746
D: 351.43847256667846
D: 381.74467907228257
D: 403.94182749499959
D: 405.28755223914783
D: 463.71219522458108
D: 505.83495331975627
D: 519.60465740791813
D: 591.93665201607507
D: 602.34375567444874
mindis: 237.01898658124415
Node:17
Source 40
DES:42
17
RN:17
Source 40
DES:42
42
Route from 41 to 42
RN:41
Source 41
DES:42
42
Enter the data to be transmitted
```



```
(x1,y1):66.0,132.0
v:23
Signature is
char:I (asci
e(3):186
Signature:23
u1:29.368421
u2:3.6315789
(x1,y1):66.0
v:23
Signature is
char:I (asci
e(4):186
Signature:23
u1:29.368421
u2:3.6315789
(x1,y1):66.0
v:23
Signature is
User ID of 2
HASH:60157
User ID of 3
HASH:126334
User ID of 4
HASH:216514
Dataitem(1):
Dataitem(2):
Dataitem(3):
Dataitem(4):
Hash Functio
Hash Functio
Hash Functio
Hash Functio
UAU:4
channel.cc:3
highestAnten
SORTING LIST
[root@home D
```

5. CONCLUSION

In this paper, we will all start a play program, taking Double Server Open Key cryptography with shibboleth Hunt methods that will wait amid a visual name attack attack associated with the weakness of the PE-KS cultural brand. We look forward to regardless of the collection brought to the flat world of Projective Hash in addition to using it to scale up the DSP-EKS uncontested strategy. The practical SP-HF's first indicator described in Diffie-Hellman's negative contexts is the most prominent in this document which provides a good DS-PEKS strategy while not limited to increasing the security of authentication data, this document makes an important effort to go authoritatively to prevent unwanted gaming server assignments.

6. REFERENCES

[1] R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, “A new general framework for secure public key encryption with keyword search,” in Proc. 20th Australasian Conf. Inf. Secure. Privacy (ACISP), 2015, pp. 59–76.

[2] P. Xu, H. Jin, Q. Wu, and W. Wang, “Public-key encryption with a fuzzy keyword search: A provably secure scheme under keyword guessing attack,” IEEE Trans. Computer., vol. 62, no. 11, pp. 2266–2277, Nov. 2013.

[3] D. Khader, “Public key encryption with keyword search based on K-resilient IBE,” in Proc. Int. Conf. Computer. Sci. Appl. (ICCSA), 2006, pp. 298–308.

[4] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: Improved definitions and efficient constructions,” in Proc. 13th ACM Conf. Computer. Commun.Secure. (CCS), 2006, pp. 79–88.\

[5] M. Abdalla et al., “Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions,” in Proc. 25th Annu. Int. Conf. CRYPTO, 2005, pp. 205–222.

[6] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, “Building an encrypted and searchable audit log,” in Proc. NDSS, 2004, pp. 1–11.

[7] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Proc. Int. Conf. EUROCRYPT, 2004, pp. 506–522.

[8] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, “Order preserving encryption for numeric data,” in Proc. ACM SIGMOD Int. Conf. Manage. Data, 2004, pp. 563–574.