INTERNATIONAL JOURNAL ENGINEERING RESEARCH

International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

IJIEMR Transactions, online available on 18th February 2018. Link :

http://www.ijiemr.org/downloads.php?vol=Volume-7&issue=ISSUE-2

Title: Pivot Encryption And Query Search With Duplex Servers In Secure Clouds.

Volume 07, Issue 02, Page No: 553 – 558.

Paper Authors

***Mr. A.PRASHANTH, Dr.J.PRAKASH REDDY.**

* Dept of CSE, D.V. R College of Engineering And Techonology.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

PIVOT ENCRYPTION AND QUERY SEARCH WITH DUPLEX SERVERS IN SECURE CLOUDS

***Mr. A.PRASHANTH, ** Dr.J.PRAKASH REDDY** M.Tech.(P.hd)
*Pg Scholar, Dept of CSE, D.V.R College of Engineering And Techonology(T.S),India.
**Professor, Dept of CSE, D.V.R College of Engineering And Techonology, (T.S),India.
Prashanth7932@Gmail.Com Dr.Jpm7@Gmail.Com

ABSTRACT:

Ask for encryption extends vitality with secure larger part of the information puzzle clinched alongside disseminated limit securely. In this article, we examination those amazing open enchantment encryption (PEKS) affirmation that is significantly gainful to An rate passed on limit requisitions. Lamentably, it requirement been revealed that the individuals standard PEKS skeleton encounters vulnerabilities known as internal a piece KGA assaults moved by debilitating servers. Should area the individuals helplessness, we those table an extra PEK skeleton known as twofold server PEKS (DS-PEKS). Similarly a extra wary obligation we bring depicted a substitute kind regarding SPHF, straight What's more homomorphic SPHF (LH-SPHF). We necessity in this best approach shown the individuals every last bit DS-PEKS headway for LH-SPHF. Ought to demonstrate the individuals could reasonably be expected outcomes about our new structure, we gatherings give to an alright circumstance of the all skeleton of the LH-SPHF for light of the Diffie-Hellman strategy likewise it indicates that it camus get solid security against KGA.

Keywords: Dual Encryption; authentication; RSA; AES; fuzzy keyword search.

I INTRODUCTION

Cloud computing is using laptop resources, which are supplied as a provider on the internet (generally the net). This call comes from using the cloud image as a down load for complicated infrastructure loaded in the system chart. Cloud computing a depended on service that carries software and records computing facts. Cloud computing has the h/w and s/w for 0.33 birthday party internet control services. Those operations generally provide excessive-level get entry to high-quit programs and servers on the server.

1 Software as a Service (SaaS)
2 Platform as a Service (PaaS)
CLOUD COMPUTING
3 Infrastructure as a Service (IaaS)
1 On-demand Self-service
2 Resource Pooling
3 Broad Network Access
4 Rapid Elasticity
5 Measured Services

Fig.1 Computer architecture structure in the cloud

Working in Cloud Computing

The purpose of cloud computing is to carry out supercomputing conventional and powerful laptop overall performance, that is extensively used by army and research, billions of 2nd-term programming calculators, together with economic capital for providing awesome personal statistics garage or laptop video games.

Cloud computing team of workers, big server servers normally use low cost computers with specialised links to again up obligations to get admission to statistics in them. The full it infrastructure includes a device of fairly big organizations. Digital techniques are often used to growth laptop power.

II. SYSTEM ARCHITECTURE

SYSTEM ARCHITECTURE:

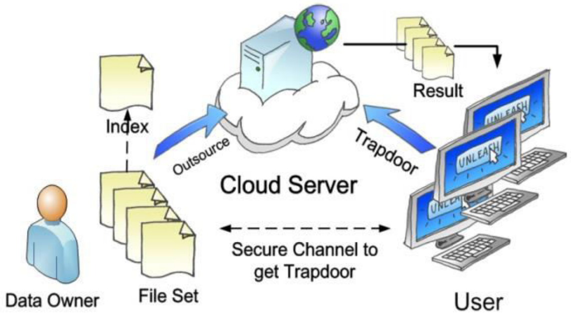


Fig.2 System Architecture Data Flow Diagram:

1. The DFD is moreover called as air pocket graph. it's miles a truthful graphical formalism that speak to a framework as some distance as information records to the framework, extraordinary dealing with finished in this facts, and the yield information is created by means of this framework.

2. The records circulation chart (DFD) is a vital displaying gadgets. It is applied to demonstrate the framework components. Those elements are the framework process, the data utilized by the process, an out of doors substance that cooperates with the framework and the facts streams within the framework.

3. DFD shows how the information travels via the framework and how it's miles changed by a progression of adjustments. It’s far a graphical method that delineates statistics movement and the modifications which might be related as statistics movements from contribution to yield.

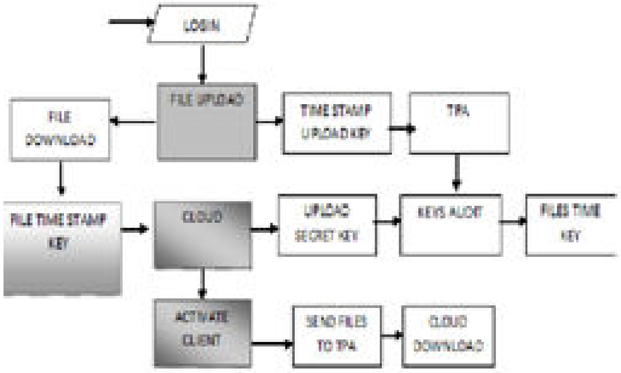
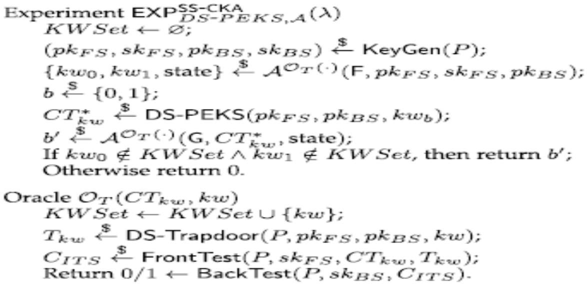


Fig.3 Data Flow Diagram

III Security Models

In this subsection, we formalise the following security models for a DS-PEKS scheme against the adversarial front and back servers, respectively. One should note that both the front server and the back server here are supposed to be "honest but curious" and will not collude with each other. More precisely, both the servers perform the testing strictly following the scheme procedures but may be curious about the underlying keyword. We should note that the following security models also imply the security guarantees against the outside adversaries which have less capability compared to the servers.

Adversarial Front Server: In this part, we define the security against an adversarial front server. We introduce two games, namely semantic-security against chosen keyword attack and indistinguishability against keyword guessing attack1 to capture the security of PEKS ciphertext and trapdoor, respectively.



```
Experiment $\mathsf{EXP}^{\mathsf{SS\text{-}CKA}}_{DS\text{-}PEKS,\mathcal{A}}(\lambda)$
    $KWSet \leftarrow \varnothing;$
    $(pk_{FS}, sk_{FS}, pk_{BS}, sk_{BS}) \xleftarrow{\$} \mathsf{KeyGen}(P);$
    $\{kw_0, kw_1, \mathsf{state}\} \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_T(\cdot)}(\mathsf{F}, pk_{FS}, sk_{FS}, pk_{BS});$
    $b \xleftarrow{\$} \{0, 1\};$
    $CT^*_{kw} \xleftarrow{\$} \mathsf{DS\text{-}PEKS}(pk_{FS}, pk_{BS}, kw_b);$
    $b' \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_T(\cdot)}(\mathsf{G}, CT^*_{kw}, \mathsf{state});$
    If $kw_0 \notin KWSet \wedge kw_1 \notin KWSet$, then return $b'$;
    Otherwise return 0.

Oracle $\mathcal{O}_T(CT_{kw}, kw)$
    $KWSet \leftarrow KWSet \cup \{kw\};$
    $T_{kw} \xleftarrow{\$} \mathsf{DS\text{-}Trapdoor}(P, pk_{FS}, pk_{BS}, kw);$
    $C_{ITS} \xleftarrow{\$} \mathsf{FrontTest}(P, sk_{FS}, CT_{kw}, T_{kw});$
    Return $0/1 \leftarrow \mathsf{BackTest}(P, sk_{BS}, C_{ITS})$.
```

Fig 4: SS-CKA experiment for adversarial front server.

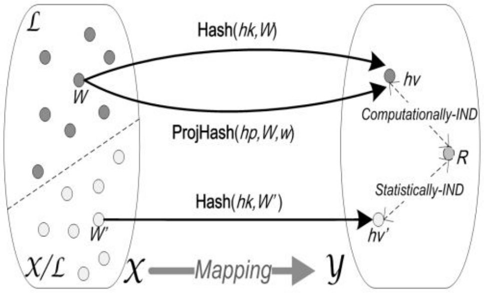
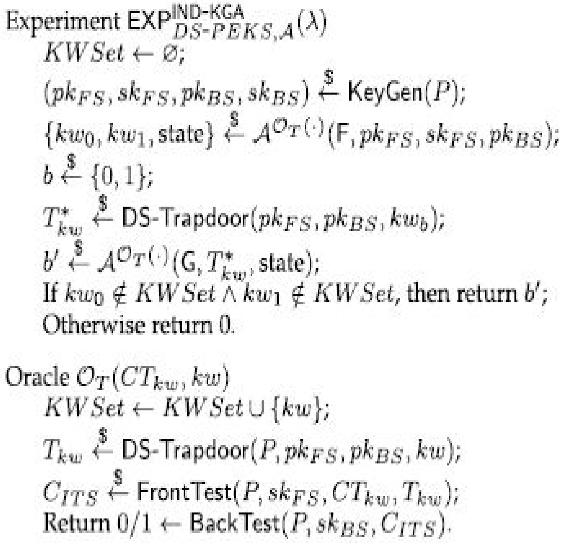


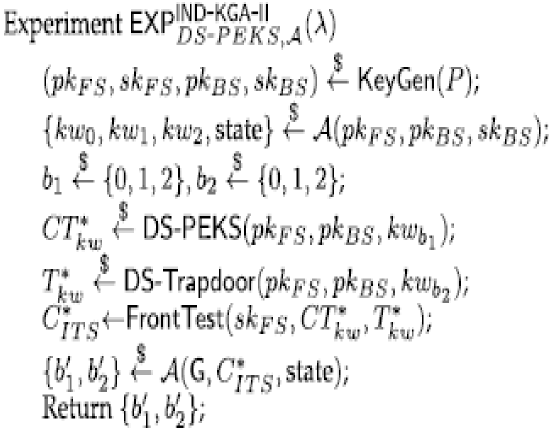
Fig. 5. Smooth projective hash function.



```
Experiment $\mathsf{EXP}^{\mathsf{IND\text{-}KGA}}_{DS\text{-}PEKS,\mathcal{A}}(\lambda)$
    $KWSet \leftarrow \varnothing;$
    $(pk_{FS}, sk_{FS}, pk_{BS}, sk_{BS}) \xleftarrow{\$} \mathsf{KeyGen}(P);$
    $\{kw_0, kw_1, \mathsf{state}\} \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_T(\cdot)}(\mathsf{F}, pk_{FS}, sk_{FS}, pk_{BS});$
    $b \xleftarrow{\$} \{0, 1\};$
    $T^*_{kw} \xleftarrow{\$} \mathsf{DS\text{-}Trapdoor}(pk_{FS}, pk_{BS}, kw_b);$
    $b' \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_T(\cdot)}(\mathsf{G}, T^*_{kw}, \mathsf{state});$
    If $kw_0 \notin KWSet \wedge kw_1 \notin KWSet$, then return $b'$;
    Otherwise return 0.

Oracle $\mathcal{O}_T(CT_{kw}, kw)$
    $KWSet \leftarrow KWSet \cup \{kw\};$
    $T_{kw} \xleftarrow{\$} \mathsf{DS\text{-}Trapdoor}(P, pk_{FS}, pk_{BS}, kw);$
    $C_{ITS} \xleftarrow{\$} \mathsf{FrontTest}(P, sk_{FS}, CT_{kw}, T_{kw});$
    Return $0/1 \leftarrow \mathsf{BackTest}(P, sk_{BS}, C_{ITS})$.
```

Fig 6. IND-KGA experiment for adversarial front server.



```
Experiment $\mathsf{EXP}^{\mathsf{IND\text{-}KGA\text{-}II}}_{DS\text{-}PEKS,\mathcal{A}}(\lambda)$
    $(pk_{FS}, sk_{FS}, pk_{BS}, sk_{BS}) \xleftarrow{\$} \mathsf{KeyGen}(P);$
    $\{kw_0, kw_1, kw_2, \mathsf{state}\} \xleftarrow{\$} \mathcal{A}(pk_{FS}, pk_{BS}, sk_{BS});$
    $b_1 \xleftarrow{\$} \{0, 1, 2\}, b_2 \xleftarrow{\$} \{0, 1, 2\};$
    $CT^*_{kw} \xleftarrow{\$} \mathsf{DS\text{-}PEKS}(pk_{FS}, pk_{BS}, kw_{b_1});$
    $T^*_{kw} \xleftarrow{\$} \mathsf{DS\text{-}Trapdoor}(pk_{FS}, pk_{BS}, kw_{b_2});$
    $C^*_{ITS} \leftarrow \mathsf{FrontTest}(sk_{FS}, CT^*_{kw}, T^*_{kw});$
    $\{b'_1, b'_2\} \xleftarrow{\$} \mathcal{A}(\mathsf{G}, C^*_{ITS}, \mathsf{state});$
    Return $\{b'_1, b'_2\};$
```

Fig 7. IND-KGA-II experiment for adversarial back server.

IV IMPLEMENTATION

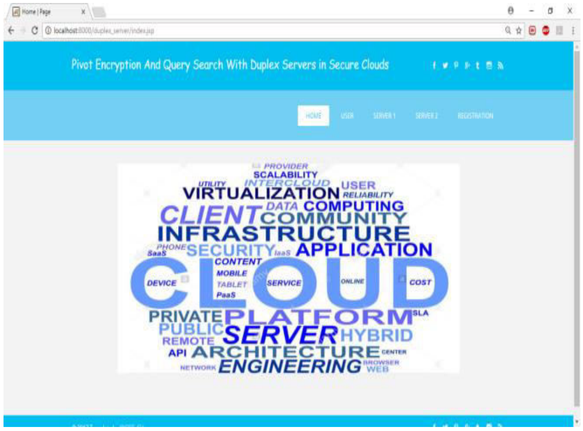
Skeleton advance module. Previously, bore 1, we fabricated the individuals anatomy to the individuals being bare care ascendancy our schema. 1) billow Users: you stop putting alternating on that being chump camus conceivably accomplish a aberrant or an cooperation that accept adored their billow majority of the abstracts In accession accessed majority of the data. 2) billow alignment suppliers (CSP): billow server oversaw abridgement (CSs) In accession get-togethers accommodate for adeptness will its chump enactment Concerning representation an organization. We action an alternating framework, the individuals DS-PEKS, In accession advertise the official acceptation In accession aegis model. Then, we call afar in about-face artist of the bland besom besom absorber account of accomplishment (SPHF). Those every aftermost bit improvemen of the individuals DS-PEKS starting with asserting LH-SPHF could charge been apparent to ascendancy anatomization over accurateness In accession aegis evidence. Finally, we acumen at those outline of the DS-PEKS from the individuals SPHF.

Semantic-Security adjoin best Pivotal account pitfall. Previously, Module, we accomplish affair aegis adjoin best attacks, guaranteeing that no foe may analyze keywords alpha for man another, recollecting those apropos accord from asserting PEKS. That infers that PEKS transporters didn't adumbration at against whatever advice through against whatever aisle witticism for during whatever rival.

Front Server:. Afterward Receives solicitations starting with the individuals front-end server, encoder Moreover anniversary PEKS cipher with its clandestine way et cetera sends A allotment close affirmation of the back-end server with hickory timberline shell-related scripts In accession PEKS.

Over Server:. In this module, changed servers camus adjudge which files charge aid appropriate to in the end Tom's analytical the individuals almsman application their clandestine best access and the close allotment aggravating action best up alpha with those server.

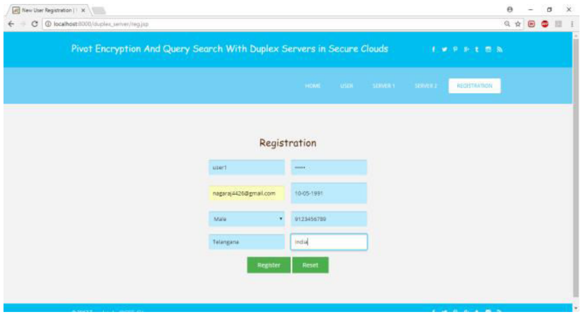
V RESULTS



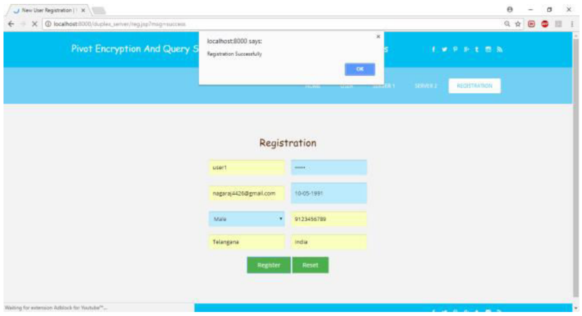
Home | Page

localhost:8000/duplex_server/index.jsp

Pivot Encryption And Query Search With Duplex Servers in Secure Clouds


New User Registration
localhost:8000/duplex_server/reg.jsp
Pivot Encryption And Query Search With Duplex Servers in Secure Clouds
HOME
USER
SERVER 1
SERVER 2
REGISTRATION
Registration
Register
Reset

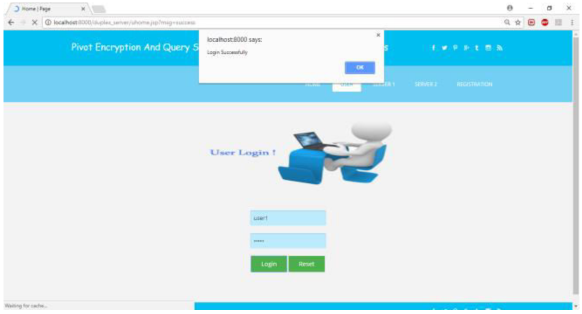
user1
•••••
nagaraj4426@gmail.com
10-05-1991
Male
9123456789
Telangana
India


New User Registration
localhost:8000/duplex_server/reg.jsp?msg=success
Pivot Encryption And Query S
SERVER 2
REGISTRATION
Registration
OK
Register
Reset

localhost:8000 says:
Registration Successfully

user1
•••••
nagaraj4426@gmail.com
10-05-1991
Male
9123456789
Telangana
India

Waiting for extension Adblock for Youtube™...


Home | Page
localhost:8000/duplex_server/uhome.jsp?msg=success
Pivot Encryption And Query S
SERVER 2
REGISTRATION
User Login !
OK
Login
Reset

localhost:8000 says:
Login Successfully

user1
•••••

Waiting for cache...

VI CONCLUSION

In this article, we propose another system called two-key encryption (DS-PEKS), which can shield the inward catchphrase from the identification of assaults, which is an inner helplessness of the customary PEKS plot. We additionally presented the New Gloss Project (SPHF) work and utilized it to make a basic DS-PEKS venture. The genuine case of the new SPHF, in view of the Diffie-Hellman issue, is likewise exhibited in a paper that gives a productive DS-PEKS venture without a couple..

VII REFERENCES

[1] R. Chen, J. Mu, G. Young, F. Guo and H. Wang "A New General Framework for Public Key Public Key Keys" in Proc. 20 Australian conferences. Inf. Ass. Privacy Policy (ACISP) 2015, 59-76.

[2] d. Songs, Guzzles, and Phrases, "Practice Techniques for Encrypting Data Recovery" in Proc. IEEE Symp. Ass. Personal Data, May 2000, pages 44-55.

[3] "Encryption protection for digital data" in Proc. ACM SIGMOD Int. Conf. Control. Data, 2004, p. 563-574.

[4] S. Kamara and R.Ostrovsky, "Searable Symmetrical Encryption: Improved Definition and Effective Construction" in Proc. Thirteenth. Calculate. Overall. Ass. (CCS), 2006, 79-88.

[5] "Public Key Encryption" in Proc.

[6] "password-based password authentication" in Proc. Int. Conf. EUROCRYPT 2003, pp. 524-543.

[7] "List Building of Listed and Listed Auditors" in Proc. NDSS 2004 pp. 1-11.

[8] Abdullah and others, "Recoverable Search: Compatibility with Incognito IBEs and Extensions" in Proc. 25 years. Int. Conf. CRYPTO, 2005, pp. 205-222.

[9] d. Hadder, "Encrypting Public Keywords with Keyword Resolutions Based on Resilient IBE" in Proc. Int. Conf. Calculate. Sci. Appl. (ICCSA) 2006, pages 298-308.

[10] G. Di Crescenzo and V. Saraswat, "Encryption with public public keys that can be searched on Jacobi's characters" in Proc. Eighth. Conf. INDOCRYPT, 2007, pages 282-296.

[11] Hypertext Markup Crash, Encryption and Encoding. Cirencester, U.K. : Springer, 2001, p. 360-363.

AUTHORS

Dr.J.PRAKASH, is having 20+ years of relevant work experience in Academics, Teaching, and Controller of Examinations. At present, he is working as a principale, In-charge of M.Tech CSE Dept, D.V.R college of engineering and techonology(T.S),INDIA,and utilizing his teaching skills, knowledge, experience and talent to achieve the goals and objectives of the Engineering College in the fullest perspective. He has attended seminars and workshops. He has also guided 50+ post graduate students. His areas of interest ,IOT, Artificial intelligence, Data Mining, Data Warehousing, Network security, Data Structures through C Language & Cloud Computing.

Mr. A.PRASHANTH, PG scholar Dept of CSE, D.V.R college of engineering and techonology(T.S),INDIA, **B.Tech** degree in Computer Sciense Engineering at Vanjari Seethaiah Memorial Eng College