# Authenticated Key Exchange Protocols for Parallel Network File Systems

C.INDUMATHI<sup>1</sup> S.MEEN<sup>2</sup> R.RAJPRIYA<sup>3</sup> N.POORNIMA<sup>4</sup> K.SUVITHA<sup>5</sup>

<sup>1</sup>(B.E (CSE), Kongunadu College of Engg & Tech, Trichy, India, kkmailit@gmail.com) <sup>2</sup>(Principal, Kongunadu College of Engg & Tech, Trichy, India)

*ABSTRACT:* In this paper, we propose a variety of authenticated key exchange protocols that are designed to address the issues. We show that our protocols are capable of reducing the workload of the metadata server and concurrently supporting forward secrecy and escrow-freeness. All this requires only a small fraction of increased computation overhead at the client. We proposed three authenticated key exchange protocols for parallel network file system (pNFS). Our protocols offer three appealing advantages over the existing Kerberos-based pNFS protocol. First, the metadata server executing our protocols has much lower workload than that of the Kerberos-based approach. Second, two our protocols provide forward secrecy: one is partially forward secure, while the other is fully forward secure. Third, we have designed a protocol which not only provides forward secrecy, but is also escrow-free.

#### KEYWORDS:

#### **INTRODUCTION**

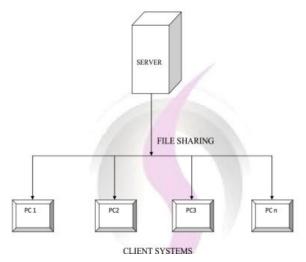
In this work, we investigate the problem of secure many to many communications in large-scale network file systems that support parallel access to multiple storage devices. That is, we consider a communication model where there are a large number of clients accessing multiple remote and distributed storage devices in parallel.

Particularly, we focus on how to exchange key materials and establish parallel secure sessions between the clients and the storage devices in the parallel Network File System (pNFS) the current Internet standard in efficient and scalable manner. The an development of pNFS is driven by Panasas, Netapp, Sun, EMC, IBM, and UMich/CITI, and

thus it shares many common features and is compatible with many existing commercial/proprietary network file systems.

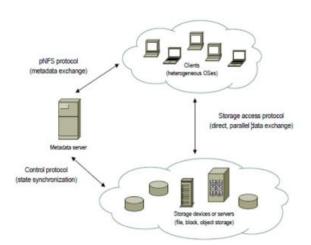
#### **EXISTING SYSTEM**

Key establishment for secure many-tomany communications. The proliferation of large-scale distributed file systems supporting parallel access to multiple storage devices. Parallel Network File System (pNFS) makes use of Kerberos to establish parallel session keys between clients and storage devices.



#### **PROPOSED SYSTEM**

Variety of authenticated key exchange protocols that are designed to address the existing issues. Protocols are capable of reducing the workload of the metadata server and concurrently supporting forward secrecy and escrow-freeness. Metadata server executing our protocols has much lower workload than that of the Kerberos-based approach.



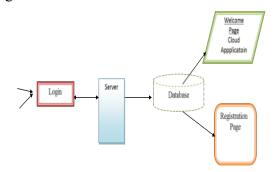
#### **MODULES**

- User Interface Design
- Parallel sessions
- Authenticated key exchange
- Forward secrecy
- Un Authorized Access

• Server Authentication

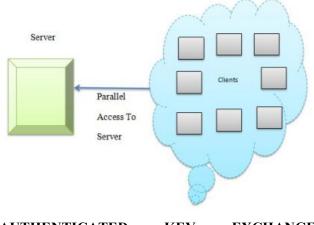
#### **USER INTERFACE DESIGN MODULE**

The important role for the Network user is to move login window to cloud user window. This module has created for the security purpose. In this login page we have to enter login user id and password. It will check username and password is match or not. If we enter any invalid username or password we can't enter into login window to user window it will shows error message. So we are preventing from unauthorized user entering into the login window to user window. It will provide a good security for our project. So server contain user id check and password server also the authentication of the user. It well improves the security and preventing from unauthorized user enters into the network. In our project we are using JSP for creating design. Here we validate the login user and sever authentication.



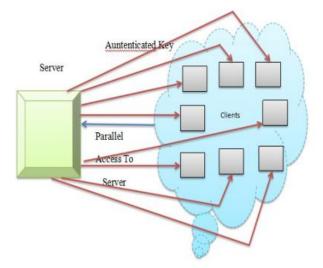
### PARALLEL SESSIONS

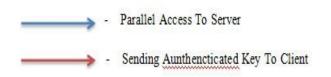
Parallel secure sessions between the clients and the storage devices in the parallel Network File System (pNFS). The current Internet standard-in an efficient and scalable manner. This is similar to the situation that once the adversary compromises the long-term secret key, it can learn all the subsequence sessions. If an honest client and an honest storage device complete matching sessions, they compute the same session key. Second, two our protocols provide forward secrecy: one is partially forward secure with respect to multiple sessions within a time period.



# AUTHENTICATED KEY EXCHANGE MODULE

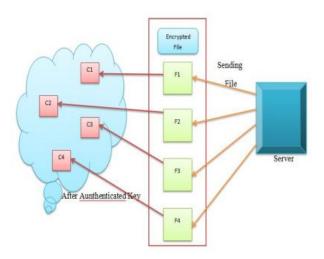
Our primary goal in this work is to design efficient and secure authenticated key exchange protocols that meet specific requirements of pNFS.The main results of this paper are three new provably secure authenticated key exchange protocols.We describe our design goals and give some intuition of a variety of pNFS authenticated key exchange6 (pNFS-AKE) protocols that we consider in this work.





### FORWARD SECRECY MODULE

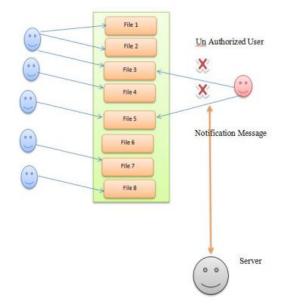
The protocol should guarantee the security of past session keys when the long-term secret key of a client or a storage device is compromised. However, the protocol does not provide any forward secrecy. To address key escrow while achieving forward secrecy simultaneously, incorporate a Diffiewe into Hellman key agreement technique Kerberos-like pNFS-AKE-I.However, note that we achieve only partial forward secrecy, by trading efficiency over security.



## **UN AUTHORIZED ACCESS**

In this module the unauthorized user i.e., the users who are not having permission to access other information. The user who uses the network in a wrong manner may block by the server when the server gets a notification message that someone is accessing in unauthorized access. Once the Unauthorized user blocked by the server cannot be undone ever.

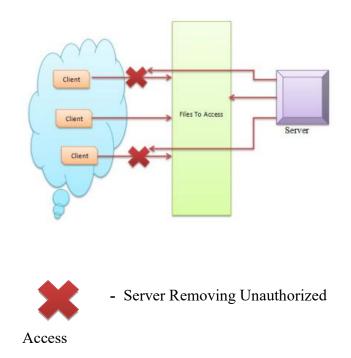
Authorized





## Accept & Allow user file:

The admin can accept the new user request and also block the users. The users can upload the file to Network. And the admin can allow the files to Network then only the file can store the cloud. If the file uploaded by the user is not permitted from the Server means the file cannot be uploaded by the Client.



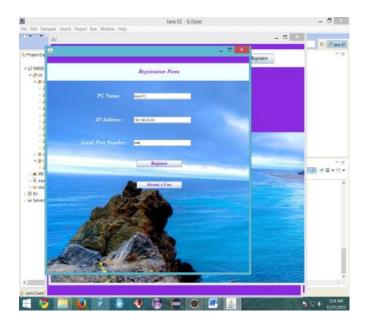
# ALGORITHM Diffie-Hellman key agreement:

Diffie-Hellman key exchange, also called exponential key exchange, is a method of digital encryption that uses numbers raised to specific powers to produce decryption keys on the basis of components that are never directly transmitted, making the task of a would-be code breaker mathematically overwhelming.

## **FUTURE ENHANCEMENT:**

Authentication using Password authenticated key exchange using distributed server (PAKEUDE) is done where a cryptographic key - exchange of messages. Security analysis has shown that our protocol is secure against passive and active attacks in case that one of the two servers is compromised.

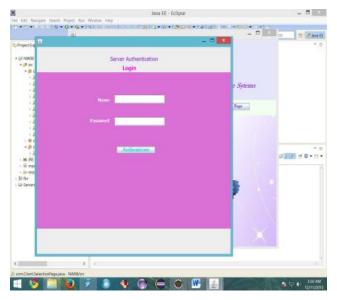
## User interface module:



**TO IDENTIFY SERVER RESPONSE:** 



**SERVER AUTHENTICATION LOGIN:** 



## **TABLES CREATIONS**

Table definitions must have a valid locator. The locator describes the real-world object that the table definition was derived from. A locator is created automatically when you import the table definition from a data source, or you can specify a locator in the Table Definition Properties window.

## TABLE FORMAT FOR KEY EXCHANGE:

				10000	e Masager					-
tid default server NetDiwelSourtere	The state									
NetOlasd Sovethine - NetwOrkEllatura			Dave in Strate Webble			logers/ansort a	poerwraeuror()	azovanij × (odave)	uegio (francalo)	Antel a 154
NetrOldenafatopero		a query Grabi	letable address Tage							
Node/Caco/Cab/Ditree	1	COLOR NO.	100 * Store 11		tal i					
NodeCostorPolacities		grante Ruse	esteta set capt	LON-Nº1						
Nodel/Victatement	8									
Nobi,Zoventere										
Nidel Serman										
Nodel:3FoutrgDate Nodel:36-Entree										
10de/IVCAddwarei										
Notelkier										
NodePortriteria in Map	- Sec.4	Munaper								
Nodes/Custom/Yopanties										
Neder/Only		AsieD	Operfaiture	P_Addeas	F_Addess_Type		UrManaged	10-Nyrajefus	ÜvMarageliHI	Cattor
NodeTettings		124	ICMP-	10.155.2.151	2.4			12/32/1008	12:55:1085	
Noder/Batetice		162	25847	10.155.8,162	194			10/35/1888	12-36/1899	
Node/Aero		186	SAMP	10.199.8.52	Red .			12/35/398	12/20/1099	
Minister Biggs	1 here	distant mental second	and the second se	A CONTRACTOR OF THE		A REAL PROPERTY.	all and the second		- OGENANT	A
halfcalother/ypw										
Notestor Namanarce/Renevala										
Nationation Type/Terressons										
MPR DescTox	1									
FR JChes										
NPR_FCRevisione										
NPR FCServers										
MRR_FCIMe										
NPH Malcuit Groatbalenets										
1978 Multi-and GroupNedas										
MPN_Malicard_Groups										
1910, Multical Group Transiation										
1792 Material Interfaces										
1Pill, Mulcast, Revolutionau/Part										
Mill Matcard RoungTable Mill Matcard RoungTable Di										
1719, Malcast, Sources	0									
NPIE, Mulcost, Sources NPIE, Mulcost/hodroptics, DAL	0									_
MME, Multiceet Sources MME, Multiceet/InutingDates CALL	0			Dátabas	e Marager		_	_		- 0
1998 MuticetholingDate DAL	0			Datatum	e Marager	_	_	_	_	- 0
MM, Malcast Sources MMM, Malcast Textropliere CAL				0.000						
Mitteeffedreptes CAL			Cest - DateMatte	n Providence	×Servedows	Nader (Nexce) a	Baselyncont	hatcheniz e Distant	ndet en (Protectes	
Million Colors C	- Europe		Ever a <b>Databased</b> er Is skile offengal Eur	el Price Chanter	x Selevitedore ()	Nader (Nexce) a	BaseviseCost	Notel Agency in State (	rdelli tr (Palificatio	
Al Affait www.	Easted 1	in sporty Enable	fa table editing . Equ	el (Hockel Andrea at to CSV - Choo	×Servedows	Nadeo(Sapercia) a	Bilevisie Con (3	katifan <u>i</u> e jiskin	rdið tri (Pulli sin	
IPR Mutcathodrotas DAL dd defailt server NedDedDormen NedDedData NedDedData NedDedData NedDedData NedDedData	t de la constante de la consta	in sporty Enable		el (Hockel Andrea at to CSV - Choo	x Selevitedore ()	Roden(Topocor) a	Bastriacher()	tablilanij a jilakiv	rdel) tr (Patricala	
Al default server Al default server NackDestDoorttee NackDestDoorttee NackDestDoorttee NackDestDoorttee NackDestDoorttee NackDestDoorttee NackDestDoorttee NackDestDoorttee NackDestDoorttee NackDestDoorttee NackDestDoorttee NackDestDoorttee NackDestDoorttee NackDestDoorttee	Easted 1	in sporty Enable	fa table editing . Equ	el (Hockel Andrea at to CSV - Choo	x Selevitedore ()	Rodenfityloxyc) a	Bielwie Oorl J	laddifianij e ji obyliv	rdið tr (žhilli dö	
UPE Matricethadrobes DAL dd defaelt server Nedback Domme Nedback Domme Nedback Domme Nedback Domme Nedback Domme Nedback	t de la constante de la consta	in sporty Enable	fa table editing . Equ	el (Hockel Andrea at to CSV - Choo	x Selevitedore ()	Nader(Taplocce) a	Balarives Devil	Notestan <u>e</u> a Balaini	nd Dan (Pallador	
Al default prover Al default prover Nacture Dourses Nacture Dourses Nacture Datas Nacture Datas	t de la constante de la consta	in sporty Enable	fa table editing . Equ	el (Hockel Andrea at to CSV - Choo	x Selevitedore ()	Nadeo[Indexce] a	Balance (	kuletiken <u>ii</u> e Dickelw	nd Davij (Palita Ace	
UPE Maturatificatir Data DAL Ad Africati Denter MatCaped Denters MacCaped Denters MacCaped Denters MacCaped Denters Noder Materials Noder Materials Noder Materials Noder Materials Noder Materials Noder Denter Noder	t de la constante de la consta	in sporty Enable	fa table editing . Equ	el (Hockel Andrea at to CSV - Choo	x Selevitedore ()	Radio(Indexce) a	Saloos Dool J	kantes) e Doahr	ndi 5 or (2 million)	
UPIN Malazerhadropfan CAL Al-Mihal serve NetCaladDaurhe NeuChthauf Vergene NeuChthauf Vergene NeuChth	t de la constante de la consta	in sporty Enable	fa table editing . Equ	el (Hockel Andrea at to CSV - Choo	x Selevitedore ()	Tado (MANCO) a	SalvisCod	katifant = (joyin'	ndi Sur (Prant dor	
HPM MalocathodropTax OAL MathathodropTax OAL MarDadDatation MarDatation	1 2 3	a query Tauli golate Room	fa table editing . Equ	el (Hockel Andrea at to CSV - Choo	x Selevitedore ()	Noderfitylosor) a	Balainte Cool J	kaletiken <u>i</u> a Diskov	ndelli nel (Frank alco	
HPM MateraffustryCare 2046 Medicatifustry Care Modified Constraint Multilated Constraint Multilated Constraint Multilated Constraint Subdit Add Sand' Mitsquatter Turket Aller Annual Multilated	1 2 3	in sporty - Enable	fa table editing . Equ	el (Hockel Andrea at to CSV - Choo	x Selevitedore ()	Nadeo(NARROCC) a	5.acros0col3	katriang a (katri	nde S en (Promotor	
HPM MatcathskryDaw OAE MatcathskryDaw OAE MatCathalan MatCathan MatCathan	1 2 3	a query local activite a const apolete Room	istikkeding lipp selate ses onjil	el Proc Gran Ang et to Civ – Char Linn – et f	k Selevitedoreji 18					Annel e Sal
HPM Materaffissiongtaw 244 Materaffissiongtaw 244 Mathematican Machana Constitution Matchana Constitution Matchana Constitution Matchana Constitution Matchana Matc	Land 1 2 3 Pand	a query Tauli golate Room	in talah editing Tapa telipaka pera capit Objectiva Type	P. jddeau	r, Solarihadore (d 190 190 190 190 190		0/Respt	12-MarageFrom	Urfange Ott	
UMI MidzaffustryDars CAE Middfust server MiddfustCountees MiddfustCountees MiddfustCountees MiddCountees Mid	1 2 3	a guary Enable golaria Robe a Managar bodal?	An table offing Tape to Do to a set of capit Opertified Type CAP	P_Addess 1015412	P,Ather,Ter	Sprence P	Urlangel	LinMaragaProse 12/30/105	Uniformational 12/08/1898	enneri = Cat
UPIL Malinashusoybas 244 M. Miharkovy McDao Duerses NacO McDau, Parasan NacO McDau, Pa	Land 1 2 3 Pand	a guery Tradi apdeba Rode Banages () Bode Sol	Gescherden Geschertige Geschertige Geb	P_Address 10 105 10	P, Altes, Ter	Sprence P	Driftmand	UrMeragePiter U.55-1016 U.55-1016	Uniformation Uniformation Table Table	enneri = Cat
HPI Matanharqtas DAL Matanharqtas DAL Matanharqtas Matanbartes Matanbartes Matanbartes Matanbartes MacAllande Matanbartes	Land 1 2 3 Pand	a guary Enable golaria Robe a Managar bodal?	An table offing Tape to Do to a set of capit Opertified Type CAP	P_Addess 1015412	P,Ather,Ter		Urlangel	LinMaragaProse 12/30/105	Uniformational 12/08/1898	enneri = Cat
PPI Mahasharqhas DAL Mahasharqhas DAL Mahasharqhasan Mahasharqhasa	Land 1 2 3 Feed	a guery Tradi apdeba Rode Banages () Bode Sol	Gescherden Geschertige Geschertige Geb	P_Address 10 105 10	P, Altes, Ter	Sprence P	Driftmand	UrMeragePiter U.55-1016 U.55-1016	Uniformation Uniformation Table Table	Annel e Sal
HPM Mahambangtas Dis Mahambangtas Magazbaran sa Magazbaran sa Magazba	Land 1 2 3 Feed	a guery Tradi apdeba Rode Banages () Bode Sol	Gescherden Geschertige Geschertige Geb	P_Address 10 105 10	P, Altes, Ter	Sprence P	Driftmand	UrMeragePiter U.55-1016 U.55-1016	Uniformation Uniformation Table Table	Annel e Sal
PPI Manafeseçüs Dil Manafeseçüs Dil	Land 1 2 3 Feed	a guery Tradi apdeba Rode Banages () Bode Sol	Gescherden Geschertige Geschertige Geb	P_Address 10 105 10	P, Altes, Ter	Sprence P	Driftmand	UrMaragePiter U.55-1016 U.55-1016	Uniformation Uniformation Table Table	Annel e Sal
Im Manufacetta Di Martin With Martin With Martin Ma	Land 1 2 3 Feed	a guery Tradi apdeba Rode Banages () Bode Sol	Gescherden Geschertige Geschertige Geb	P_Address 10 105 10	P, Altes, Ter	Sprence P	Driftmand	UrMaragePiter U.55-1016 U.55-1016	Uniformation Uniformation Table Table	Annel e Sal
IPP Manasharaptas Dis Al Alfaal tarve Status S	Level 1 2 1	a guery Tradi apdeba Rode Banages () Bode Sol	Gescherden Geschertige Geschertige Geb	P_Address 10 105 10	P, Altes, Ter	Sprence P	Driftmand	UrMaragePiter U.55-1016 U.55-1016	Uniformation Uniformation Table Table	enneri = Cat
PPI Mitoshisegita Dil Mitoshiwe	Level 1 2 1	a guery Tradi apdeba Rode Banages () Bode Sol	Gescherden Geschertige Geschertige Geb	P_Address 10 105 10	P, Altes, Ter	Sprence P	Driftmand	UrMaragePiter U.55-1016 U.55-1016	Uniformation Uniformation Table Table	enneri = Cat
HPI Mitcaribacetta Di Martalia vivi walacticento tastacticento t	Level 1 2 1	a guery Tradi apdeba Rode Banages () Bode Sol	Gescherden Geschertige Geschertige Geb	P_Address 10 105 10	P, Altes, Ter	Sprence P	Driftmand	UrMaragePiter U.55-1016 U.55-1016	Uniformation Uniformation Table Table	enneri = Cat
Markenbergen Die Markenbergen Die Markenbergen Markenberg	Level 1 2 1	a guery Tradi apdeba Rode Banages () Bode Sol	Gescherden Geschertige Geschertige Geb	P_Address 10 105 10	P, Altes, Ter	Sprence P	Driftmand	UrMaragePiter U.55-1016 U.55-1016	Uniformation Uniformation Table Table	enneri = Cat
Inthe Management (Management) Al Affaith wave wave     All Affaith wave     All Affaith wave     All Affaith wave     All Affaith affaith     Read-Affaith     Re	Level 1 2 1	a guery Tradi apdeba Rode Banages () Bode Sol	Gescherden Geschertige Geschertige Geb	P_Address 10 105 10	P, Altes, Ter	Sprence -	Driftmand	UrMaragePiter U.55-1016 U.55-1016	Uniformation Uniformation Table Table	enneri = Cat
Im Manufikenetika Oli Manufikenetika Oli Marka New Manufikenetika Ma	Level 1 2 1	a guery Tradi apdeba Rode Banages () Bode Sol	Gescherden von	P_Address 10 105 10	P, Altes, Ter	Sprence -	Driftmand	UrMaragePiter U.55-1016 U.55-1016	Uniformation Uniformation Table Table	enneri = Cat
Hith Materialsactics Di Materialsactics Di Markatowe Ma	Level 1 2 1	a guery Tradi apdeba Rode Banages () Bode Sol	Gescherden von	P_Address 10 105 10	P, Altes, Ter	Sprence -	Driftmand	UrMaragePiter U.55-1016 U.55-1016	Uniformation Uniformation Table Table	enneri = Cat
Hith Managements of the Managements of the Management	Level 1 2 1	a guery Tradi apdeba Rode Banages () Bode Sol	Gescherden von	P_Address 10 105 10	P, Altes, Ter	Sprence -	Driftmand	UrMaragePiter U.55-1016 U.55-1016	Uniformation Uniformation Table Table	enneri = Cat
Im Manufikenetika Oli Manufikenetika Oli Marka New Manufikenetika Ma	Level 1 2 1	a guery Tradi apdeba Rode Banages () Bode Sol	Gescherden von	P_Address 10 105 10	P, Altes, Ter	Sprence -	Driftmand	UrMaragePiter U.55-1016 U.55-1016	Uniformation Uniformation Table Table	enneri = Cat
Hith Managemene (M) Alexan Anno (M) Alexan Anno(M) Alexan Anno (M) Alexan Anno (M) Alexan Anno (M)	Level 1 2 1	a guery Tradi apdeba Rode Banages () Bode Sol	Gescherden von	P_Address 10 105 10	P, Altes, Ter	Sprence -	Driftmand	UrMaragePiter U.55-1016 U.55-1016	Uniformation Uniformation Table Table	enneri = Cat
Mituative Constraints Advancement	Level 1 2 1	a guery Tradi apdeba Rode Banages () Bode Sol	Gescherden von	P_Address 10 105 10	P, Altes, Ter	Sprence -	Driftmand	UrMaragePiter U.55-1016 U.55-1016	Uniformation Uniformation Table Table	enneri = Cat
Hit Manufaseria Di Manufaseria Di Manufaseria Di Manufaseria	Level 1 2 1	a guery Tradi apdeba Rode Banages () Bode Sol	Gescherden von	P_Address 10 105 10	P, Altes, Ter	Sprence -	Driftmand	UrMaragePiter U.55-1016 U.55-1016	Uniformation Uniformation Table Table	enneri = Cat
Hit Manual and A Dia Manual Annual A Dia Marka Manual A D	Level 1 2 1	a guery Tradi apdeba Rode Banages () Bode Sol	Gescherden von	P_Address 10 105 10	P, Altes, Ter	Sprence -	Driftmand	UrMaragePiter U.55-1016 U.55-1016	Uniformation Uniformation Table Table	enneri = Cat
Hit Manufaseria Di Manufaseria Di Manufaseria Di Manufaseria	Level 1 2 1	a guery Tradi apdeba Rode Banages () Bode Sol	Gescherden von	P_Address 10 105 10	P, Altes, Ter	Sprence -	Driftmand	UrMaragePiter U.55-1016 U.55-1016	Uniformation Uniformation Table Table	enneri = Cat

## **CONCLUSION**

We proposed three authenticated key exchange protocols for parallel network file system (pNFS). Our protocols offer three appealing advantages over the existing Kerberos-based pNFS protocol. First, the metadata server executing our protocols has much lower workload than that of the Kerberosbased approach. Second, two our protocols provide forward secrecy: one is partially forward secure (with respect to multiple sessions within a time period), while the other is fully forward secure (with respect to a session). Third, we have designed a protocol which not only provides forward secrecy, but is also escrow-free.

## REFERENCES

[1] A. Zouaq and R. Nkambou, "Evaluating the Generation of Domain Ontologies in the Knowledge Puzzle Project," IEEE Trans. Knowledge and Data Eng., vol. 21, no. 11, pp. 1559-1572, Nov. 2009.

[2] A. Maedche and S. Staab, "Ontology Learning for the Semantic Web," IEEE Intelligent Systems, vol. 16, no. 2, pp. 72-79, Mar. 2001.

[3] P. Velardi, R. Navigli, A. Cucchiarello, and F. Neri, "Evaluation of Onto Learn, a Methodology for Automatic Learning of Domain Ontology's," Ontology Learning from Text: Methods, Applications, and Evaluation, P. Buitelaar, P. Cimiano, and B. Magnini, eds., pp. 92-106, IOS Press, 2005..

[4] A. Conde, M. Larran<sup>~</sup> aga, I. Calvo, J.A. Elorriaga, and A. Arruarte, "Automating the Authoring of Learning Material in Computer Engineering Education," Proc. 42nd IEEE Frontiers in Education Conf. (FIE '12), pp. 1376-1381, 2012.

[5] "Constraint Grammar: Language-Independent System for Parsing Unrestricted Text," Natural Language Processing, F.Karlsson, A. Voutilainen, and J. Heikkila, eds., no. 4, Mouton de Gruyter, 1995.

[6] T. Leidig, "L3-Towards an Open Learning Environment," ACM J. Educational Resources in Computing, vol. 1, no. 1, pp. 5-11, 2001.

[7] P. Vossen, "Extending, Trimming and Fusing WordNet for Technical Documents," Proc. Second Meeting of the North Am. Chapter of the Assoc. for Computational Linguistics (NAACL '01), 2001.

[8] K. Verbert, D. Ga\_sevi\_c, J. Jovanovi\_c, and E. Duval, "Ontology- Based Learning abContent Repurposing," Proc. 14th Int'l Conf. World Wide Web (WWW '05), pp. 1140-1141, 2005.

[9] M. Larran<sup>~</sup>aga, I. Niebla, U. Ruedat, J.A. Elorriaga, and A.Arruarte, "Towards Collaborative Domain Module Authoring," Proc. Seventh IEEE Int'l Conf. Advanced Learning Technologies (ICALT '07), pp. 814-818, July 2007.

[10] K. Cardinaels, M. Meire, and E. Duval, "Automating Metadata Generation: The Simple Indexing Interface," Proc. 14th Int'l Conf. World Wide Web (WWW '05), 2005.