



VIGNANA BHARATHI
Institute of Technology®

(A UGC Autonomous Institution, Approved by AICTE, Accredited by NBA & NAAC-A Grade, Affiliated to JNTUH)

(Sponsored by Swamy Vivekanda Educational Trust, Hyd.)

CERTIFICATE

FILE AND LINK No: MRP-6943/16 (SERO/UGC)

NAME OF THE PRINCIPAL INVESTIGATOR: G.K. Karthika

Vignana Bharathi Institute of Technology,

Aushapur, Hyderabad, Pin: 501301

TITLE OF THE PROJECT: Cryptographic key exchange using two server PAKE”,

Certified that the project has been successfully completed and Executive summary of the report, Research documents, monograph, academic papers published under Minor research project has been posted on the website of the college

Signature of the Principal Investigator

Signature of the Principal
With seal and stamp

PRINCIPAL

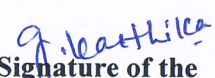
Vignana Bharathi Institute of Technology
Aushapur(V), Ghatkesar(M), Medchal Dist-501 301





ACCESSION CERTIFICATE

This is to certified that G.K.Karthika, Department of Information Technology, Hyderabad has handed over the following books and journals purchased under the scheme of Minor Research Project to the Library of Vignana Bharathi Institute of Technology, Hyderabad. The following are books and journals handed over by G.K.Karthika (MRP-6943/16 (UGC/SERO)).

S. No	Item	Qty.
1	Express Learning Cryptography and Network security	1
2	Mastering active directory	1
3	Cryptography and Network security by Forouzan	1
4	Cryptography and Network security- Principles and Practice	1
5	Cryptography and Network security by Atul Kahate	1
6	Big data Storage,sharing and security	1
7	Introduction to computer and network security	1
8	Introduction to modern cryptography	1
9	Cyberspace and cyber security	1
10	Understanding and applying cryptography and data security	1
11	Applied Cryptography protocols, algorithms and source code in c	1
12	Handbook of applied cryptography	1
13	Understanding cryptography : A T B for students and practitioners	1
14	Network security test lab step by step	1
15	Cryptography and network security	1


Signature of the
Principal Investigator



Signature of the
Librarian
SRINIVASA RAO GANTA
Asst. Professor in LIS
& Librarian VBIT



Signature of the
Principal
PRINCIPAL
Vignana Bharathi Institute of Technology
Aushapur(V), Ghatkesar(M), Medchal Dist-501 301

ASSETS CERTIFICATE

This is to certified that G.K.Karthika, Department of Information Technology, Hyderabad has handed over the following equipment purchased under the scheme of Minor Research Project to the Department of Information Technology, Vignana Bharathi Institute of Technology, Hyderabad. The following are equipments handed over by G.K.Karthika (MRP-6943/16 (UGC/SERO)).

S. No	Particulars	Company	Qty.
1	HP 15BR LAPTOP	HP	1
2	HP BACKPACK	HP	1
3	COLOR LASERJET	HP	1


Signature of the
Principal Investigator


Signature of the
Head of the Dept.
Vignana Bharathi Institute of Technology
Aushapur Vill: Ghatkesar Mdl: R R Dist -501 301


Signature of the
Principal
PRINCIPAL
Vignana Bharathi Institute of Technology
Aushapur(V), Ghatkesar(M), Medchal Dist-501 301

Settlement proforma

UTILISATION CERTIFICATE

FILE AND LINK No: MRP-6943/16 (SERO/UGC)

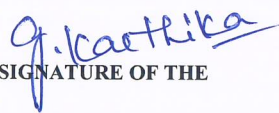
NAME OF THE PRINCIPAL INVESTIGATOR: G.K.Karthika


Vignana Bharathi Institute of Technology,

Aushapur, Hyderabad, Pin: 501301

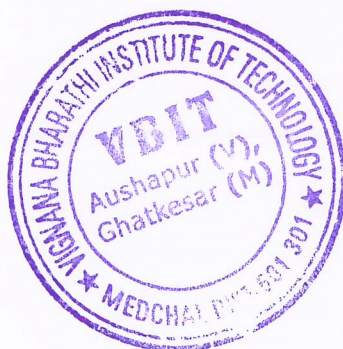
TITLE OF THE PROJECT: "Cryptographic Key Exchange Using Two Servers PAKE",

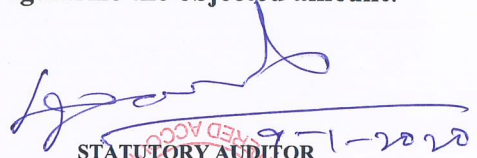
Certified that the grant of Rs. 2,40,000/ (Rupees Two lakh forty thousand only) approved by UGC and the grant received Rs2,31,000/(Rupees Two lakh Thirty One thousand only) from the University Grants Commission under the scheme of support for Minor Research Project entitled "Cryptographic Key Exchange Using Two Servers PAKE", vide UGC letter No. F.MRP-6943/16 (SERO/UGC) dated 28/7/2017 has been fully utilized for the purpose for which it was sanctioned and that the balance of Rs.9000 has been spent by institute which has to be released from UGC in accordance with the terms and conditions laid down by the University Grants Commission. If as a result of check or audit objection, some irregularity is noticed at a later stage, action will be taken to refund or regularize the objected amount.


SIGNATURE OF THE
PRINCIPAL INVESTIGATOR


PRINCIPAL with
Seal and
Stamp

PRINCIPAL
Vignana Bharathi Institute of Technology
Aushapur(V), Ghatkesar(M), Medchal Dist-501 301




STATUTORY AUDITOR
with Seal and Stamp

CA. L. JANARDHAN RAO
Chartered Accountant
M.No: 18474

UDIN: 20018474AAAAAH8371

Annexure - III

**UNIVERSITY GRANTS COMMISSION
BAHADUR SHAH ZAFAR MARG
NEW DELHI – 110 002**

**STATEMENT OF EXPENDITURE IN RESPECT OF MINOR RESEARCH PROJECT
(II Year)**

- 1.Name of Principal Investigator : G.K.Karthika₁
- 2.Dept of PI : Information Technology
- Name of College : Vignana Bharathi Institute of Technology
- 3.UGC approval Letter No. and Date : TLRA00000269, 2-Aug-2017 , MRP-6943/16
(SERO/UGC)
- 4.Title of the Research Project : Cryptographic Key Exchange Authentication UsingTwo
Servers PAKE
- 5.Effective date of starting the project:8-Aug-2017
- 6.a. Period of Expenditure: From :04-jan-2019to 07-Aug-2019
- b. Details of Expenditure

S.No.	Item	Amount Approved (Rs.)	Amount Received (Rs.)	Expenditure Incurred (Rs.)	Amount to be released by UGC
i.	Books & Journals	00	00	00	00
ii.	Equipment	00	00	00	00
iii.	Contingency including special needs	15000	12000	15000	3000
iv.	Field Work/Travel (Give details in the proform) a .	15000	12000	15000	3000
v.	Hiring Services	15000	12000	15000	3000
GRAND TOTAL		45,000	36000	45,000	9,000

7. if as a result of check or audit objection some irregularity is noticed at later date, action will be taken to refund, adjust or regularize the objected amounts.

8. It is certified that the grant of Rs. **45,000/-** (Rupees Forty Five thousand only) approved by UGC and the grant received Rs. **36,000/-** from the University Grants Commission under the scheme of support for Minor Research Project entitled Cryptographic Key Exchange Using Two Servers PAKE UGC letter No. F MRP-6943/16 (SERO/UGC) **dated 8-Aug-2017** has been fully utilized for the purpose for which it was sanctioned and that the balance of Rs. **9000** has been spent by institute which has to be released from UGC in accordance with the terms and conditions laid down by the University Grants Commission.


SIGNATURE OF PRINCIPAL INVESTIGATOR


PRINCIPAL
PRINCIPAL
Vignana Bharathi Institute of Technology
Aushapur(V), Ghatkesar(M), Medchal Dist-501 301

(Seal)



Annexure - V

UNIVERSITY GRANTS COMMISSION
BAHADUR SHAH ZAFAR MARG
NEW DELHI – 110 002

Utilization certificate(II YEAR)

Certified that the grant of Rs. **45,000/** (Rupees Forty five thousand only) approved by UGC and the grant received RS **36,000**(Rupees Thirty Six thousand only) from the University Grants Commission under the scheme of support for Minor Research Project entitled "Cryptographic Key Exchange Using Two Servers PAKE" vide UGC letter No. F. MRP-6943/16 (SERO/UGC) dated **8-Aug-2017** has been fully utilized for the purpose for which it was sanctioned and that the balance of Rs. **9000** has been spent by institute which has to be released from UGC in accordance with the terms and conditions laid down by the University Grants Commission

g. karthika
SIGNATURE OF THE
PRINCIPAL INVESTIGATOR

2
PRINCIPAL
PRINCIPAL

Vignana Bharathi Institute of Technology
Aushapur(V), Ghatkesar(M), Medchal Dist-501 301
(Seal)



g. karthika
STATUTORY AUDITOR

9-1-2020



CA. L. JANARDHAN RAO
Chartered Accountant
M.No: 18474

UDIN: 20018474AAAAH8371

Annexure - III

**UNIVERSITY GRANTS COMMISSION
BAHADUR SHAH ZAFAR MARG
NEW DELHI – 110 002**

**STATEMENT OF EXPENDITURE IN RESPECT OF MINOR RESEARCH PROJECT
(Consolidated I&II YEAR)**

1. Name of Principal Investigator : G.K.Karthika.
2. Dept of PI : Information Technology
Name of College : Vignana Bharathi Institute of Technology
3. UGC approval Letter No. and Date : TLRA00000269, 2-Aug-2017 , MRP-6943/16
(SERO/UGC)
4. Title of the Research Project : Cryptographic Key Exchange Authentication Using Two Servers PAKE
5. Effective date of starting the project: 8-Aug-2017
6. a. Period of Expenditure: From : 04-jan-2019 to 07-Aug-2019
b. Details of Expenditure

S.No.	Item	Amount Approved (Rs.)	Amount Received (Rs.)	Expenditure Incurred (Rs.)	Amount to be released by UGC
i.	Books & Journals	30000	30000	30000	00
ii.	Equipment	120000	120000	120000	00
iii.	Contingency including special needs	30000	27000	30000	3000
iv.	Field Work/Travel (Give details in the proform) a .	30000	27000	30000	3000
v.	Hiring Services	30000	27000	30000	3000
GRAND TOTAL		2,40,000	2,31,000	2,40,000	9,000

7. if as a result of check or audit objection some irregularly is noticed at later date, action will be taken to refund, adjust or regularize the objected amounts.

8. It is certified that the grant of Rs. 2,40,000/ (Rupees Two lakh Forty thousand only) approved by UGC and the grant received Rs.2,31,000/- from the University Grants Commission under the scheme of support for Minor Research Project entitled Cryptographic Key Exchange Using Two Servers PAKE UGC letter No. F MRP-6943/16 (SERO/UGC) **dated 8-Aug-2017** has been fully utilized for the purpose for which it was sanctioned and that the balance of Rs.**9000** has been spent by institute which has to be released from UGC in accordance with the terms and conditions laid down by the University Grants Commission.


SIGNATURE OF PRINCIPAL INVESTIGATOR


PRINCIPAL
Vignana Bharathi Institute of Technology
Aushapur(V), Ghatkesar(M), Medchal Dist-501 301

(Seal)



Annexure - IV

**UNIVERSITY GRANTS COMMISSION
BAHADUR SHAH ZAFAR MARG
NEW DELHI – 110 002**

STATEMENT OF EXPENDITURE INCURRED ON FIELD

WORK Name of the Principal Investigator: G.K.Karthika

Name of the Place visited	Duration of the Visit		Purpose	Mode of Journey	Expenditure Incurred (Rs.)
	From	To			
RCI Kanchanbagh	4-7-2019	6-7-2019	To discuss the usage of technology	Hired cab	5500.00
RCI Kanchanbagh	18-7-2019	19-7-2019	Practical implementation	Hired cab	3000.00
RCI Kanchanbagh	26-7-2019	29-7-2019	Discussed the final results in details and modification of context	Hired cab	6500.00
Grand Total					15,000.00

Certified that the above expenditure is in accordance with the UGC norms for Major Research Projects.

G. Karthika.
SIGNATURE OF PRINCIPAL INVESTIGATOR

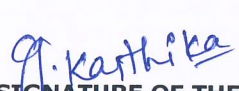
[Signature]
PRINCIPAL
(Seal)
PRINCIPAL
Vignana Bharathi Institute of Technology
Aushapur(V), Chatkesari(N), Medchal Dist-501 301

Annexure - V

UNIVERSITY GRANTS COMMISSION
BAHADUR SHAH ZAFAR MARG
NEW DELHI – 110 002

Utilization certificate(I &II YEAR)

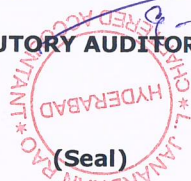
Certified that the grant of Rs.2,40,000/ (Rupees Two Lakh forty thousand only) approved by UGC and the grant received RS 2,31,000(Rupees Two Lakh Thirty one thousand only) from the University Grants Commission under the scheme of support for Minor Research Project entitled "Cryptographic Key Exchange Using Two Servers PAKE" vide UGC letter No. F. MRP-6943/16 (SERO/UGC) dated **8-Aug-2017** has been fully utilized for the purpose for which it was sanctioned and that the balance of Rs.**9000** has been spent by institute which has to be released from UGC in accordance with the terms and conditions laid down by the University Grants Commission


SIGNATURE OF THE
PRINCIPAL INVESTIGATOR


PRINCIPAL
Vignana Bharathi Institute of Technology
Aushapur(V), Ghatkesar(M), Medchal Dist-501 301
(Seal)




STATUTORY AUDITOR


CA. L. JANARDHAN RAO
Chartered Accountant
M.No: 18474

UDIN:20018474 AAAAA+8371

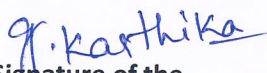
DETAILED STATEMENT OF EXPENDITURE FOR FIELDWORK & TRAVEL(II Year)

UGC Reference No. F: MRP-6943/16 (SERO/UGC)


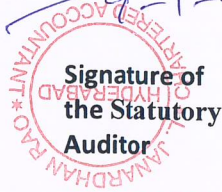
Name of the Principal Investigator: G.K.Karthika

Title of research project: "Cryptographic Key Exchange Using Two Servers PAKE"

Name of the Place visited	Duration of the Visit		Bill No	Mode of Journey	Expenditure Incurred (Rs.)
	From	To			
RGI Kanchanbagh	4-7-2019	6-7-2019	1859 0582	Hired cab	5500.00
RGI Kanchanbagh	18-7-2019	19-7-2019	018	Hired cab	3000.00
RGI Kanchanbagh	26-7-2019	29-7-2019	1860 10581	Hired cab	6500.00
Grand Total					15,000.00


Signature of the
Principal Investigator


Signature of the
Principal
PRINCIPAL
Vignana Bharathi Institute of Technology
Aushapur(V), Ghatkesar(M), Medchal Dist-501 301


Signature of
the Statutory
Auditor

CA. L. JANARDHAN RAO
Chartered Accountant
M.No: 18474

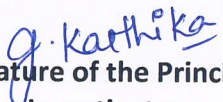
DETAILED STATEMENT OF EXPENDITURE FOR CONTINGENCY (incl. Special needs) (II YEAR)

UGC Reference No. F: MRP-6943/16 (SERO/UGC)

Name of the Principal Investigator: G.K. Karthika


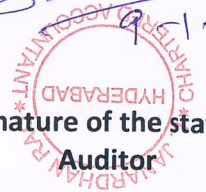
Title of research project: "Cryptographic Key Exchange Using Two Servers PAKE"

S.No	Item	Bill.No.	Date	Amount
1	Reprographic work		30-7-2019	10,000.00
2	Stationary		15-6-2019	3000.00
3	Miscellaneous (Secretarial work)		8-6-2019	500.00
4	Photostat, spiral binding		25-7-2019	1500.00
	GRAND TOTAL			15,000.00


Signature of the Principal
Investigator


Signature of the
Principal
PRINCIPAL

Vignana Bharathi Institute of Technology
Aushapur(V), Ghatkesar(M), Medchal Dist-501 301


Signature of the statutory
Auditor

CA. L. JANARDHAN RAO
Chartered Accountant
M.No: 18474

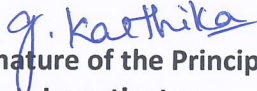
DETAILED STATEMENT OF EXPENDITURE FOR HIRING SERVICES (11 YEAR)

UGC Reference No. F: MRP-6943/16(SERO/ UGC)

Name of the Principal Investigator: G.K.Karthika

Title of research project: "Cryptographic Key Exchange Using Two Servers PAKE"

S.No	Item	Period	Bill	Date	Amount
1	Hiring services	6Months	receipt	30-7-2019	7,500.00
2	Hiring services	6Months	receipt	30-7-2019	7,500.00
	GRAND TOTAL				15,000.00


Signature of the Principal
Investigator


Signature of the
Principal

PRINCIPAL

Vignana Bharathi Institute of Technology
Kushapur(V), Ghatkesar(M), Medchal Dist-501 301


Signature of the statutory
Auditor

CA. L. JANARDHAN RAO
Chartered Accountant
M.No: 18474


DETAILED STATEMENT OF EXPENDITURE FOR FIELDWORK & TRAVEL(I&II Year)

UGC Reference No. F: MRP-6943/16 (SERO/UGC)

Name of the Principal Investigator: G.K.Karthika


Title of research project: "Cryptographic Key Exchange Using Two Servers PAKE"

Name of the Place visited	Duration of the Visit		Bill No	Mode of Journey	Expenditure Incurred (Rs.)
	From	To			
ICICI Securities - sainikpuri	18-06-2018	18-06-2018	017	Hired cab	900.00
Sambodh tex solutions - gachibowli	20-06-2018	20-06-2018		Hired cab	2850.00
Osmania university	21-06-2018	21-06-2018		Hired cab	1050.00
Jntuh University	22-06-2018	22-06-2018		Hired cab	2700.00
ICICI Securities - sainikpuri	23-07-2018	23-07-2018	021	Hired cab	900.00
Sambodh tex solutions - gachibowli	24-07-2018	24-07-2018		Hired cab	2850.00
Osmania university	25-07-2018	25-07-2018		Hired cab	1050.00
Jntuh University	26-07-2018	26-07-2018		Hired cab	2700.00
RGI Kanchanbagh	4-7-2019	6-7-2019	1859 0582	Hired cab	5500.00
RGI Kanchanbagh	18-7-2019	19-7-2019	018	Hired cab	3000.00
RGI Kanchanbagh	26-7-2019	29-7-2019	1860 10581	Hired cab	6500.00
GRAND TOTAL					30,000.00


Signature of the
Principal Investigator


Signature of the
Principal
PRINCIPAL

Anna Bharathi Institute of Technology
[V], Ghatkesar(M), Medchal Dist-501 301


Signature of
the Statutory
Auditor
CA. L. JANARDHAN RAO
Chartered Accountant
M.No: 18474

CA. L. JANARDHAN RAO
Chartered Accountant
M.No: 18474

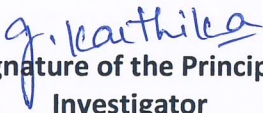
DETAILED STATEMENT OF EXPENDITURE FOR HIRING SERVICES(I&II Year)

UGC Reference No. F: MRP-6943/16(SERO/ UGC)


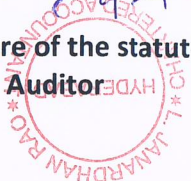
Name of the Principal Investigator: G.K.Karthika

Title of research project: "Cryptographic Key Exchange Using Two Servers PAKE"

S.No	Item	Period	Bill	Date	Amount
1	Hiring services	6Months	receipt	02-06-18	7,500.00
2	Hiring services	6Months	receipt	08-06-18	7,500.00
3	Hiring services	6Months	receipt	30-7-2019	7,500.00
4	Hiring services	6Months	receipt	30-7-2019	7,500.00
	GRAND TOTAL				30,000.00


Signature of the Principal
Investigator


Signature of the
Principal
PRINCIPAL
Vignana Bharathi Institute of Technology
Aushapur(V), Ghatkesar(M), Medchal Dist-501 301


Signature of the statutory
Auditor

CA. L. JANARDHAN RAO
Chartered Accountant
M.No: 18474

**UNIVERSITY GRANTS COMMISSION
BAHADUR SHAH ZAFAR MARG
NEW DELHI – 110 002.**

**Annual/Final Report of the work done on the Minor Research Project.
(Report to be submitted within 6 weeks after completion of each year)**


1. Project report No. 1st /Final : 2/Final
2. UGC Reference No.F. : MRP 6943/16 (SERO/UGC)
3. Period of report: from : 8-Aug-2018 to 7-Aug-2019
4. Title of research project : Cryptographic Key Exchange
Authentication Using Two Servers PAKE
5. (a) Name of the Principal Investigator : G.K.Karthika
(b) Deptt. : Information Technology
(c) College where work has progressed: Vignana Bharathi Institute of Technology
6. Effective date of starting of the project: 8-Aug-2017
7. Grant approved and expenditure incurred during the period of the report:
 - a. Total amount approved : Rs. 2.40,000
 - b. Total expenditure : Rs. 2.40,000
 - c. Report of the work done: (Please attach a separate sheet)
 - i. Brief objective of the project : (Attached)
 - ii. Work done so far and results achieved and publications, if any, resulting from the work (Give details of the papers and names of the journals in which it has been published or accepted for publication)


8. 1. Published a paper "Cryptographic Key Exchange Using Two Servers PAKE"

. Has the progress been according to original plan of work and towards achieving

iv. please enclose a summary of the findings of the study. One bound copy of the final report of work done may also be sent to the concerned Regional Office of the UGC.

v. Any other information


SIGNATURE OF THE PRINCIPAL INVESTIGATOR


PRINCIPAL
Vignana Bharathi Institute of Technology
Aushapur(V), Ghatkesar(M), Medchal Dist-501 301



UNIVERSITY GRANTS
COMMISSION BAHADUR SHAH
ZAFAR MARG NEW DELHI –
110 002

PROFORMA FOR SUBMISSION OF INFORMATION AT THE TIME OF
SENDING THE FINAL REPORT OF THE WORK DONE ON THE
PROJECT

1. Title of the Project: "Cryptographic Key Exchange Authentication Using Two Servers PAKE"

2. NAME AND ADDRESS OF THE PRINCIPAL INVESTIGATOR: G.K.Karthika, VBIT, Hyderabad.

3. NAME AND ADDRESS OF THE INSTITUTION: Vignana Bharathi Institute of Technology, Aushapur, Hyderabad

4. UGC APPROVAL LETTER NO. AND DATE: MRP-6943/16 (SERO/UGC), 28/7/2017

5. DATE OF IMPLEMENTATION: 7/08/2017

6. TENURE OF THE PROJECT: Two years

7. TOTAL GRANT ALLOCATED: 2,40,000/-

8. TOTAL GRANT RECEIVED: 2,31,000/-

9. FINAL EXPENDITURE: 2,40,000/-

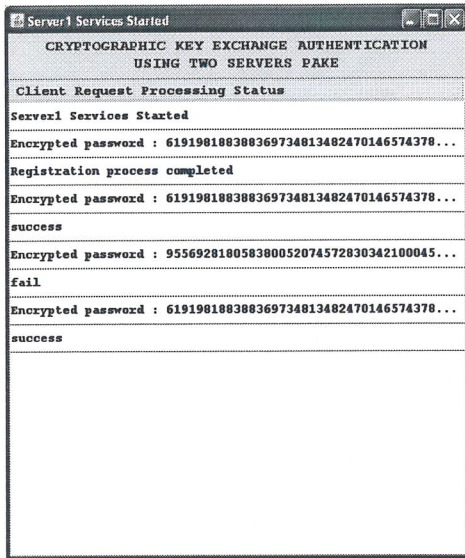
10. TITLE OF THE PROJECT: "Cryptographic Key Exchange Authentication Using Two Servers PAKE"

11. OBJECTIVES OF THE PROJECT:

- The main objective of Two Server Password-authenticated key exchange protocol is to provide Security against passive and active attacks in case that one of the two servers is compromised.
- Performance analysis has shown that our protocol is more efficient than existing symmetric and asymmetric two-server PAKE protocols in terms of parallel computation and also it takes less communication rounds.
- In addition to the efficiency the authentication and key exchange should be completed within a time limit. Hence, the protocol is secure against replay attacks.

12. WHETHER OBJECTIVES WERE ACHIEVED: YES

SUMMARY OF THE FINDINGS



After switchover the call continues this application is useful whenever there is more signal fluctuations happened when there is an important conversation call will not be terminated rather it smart call forwarded with another sim from present handset.

CONTRIBUTION TO THE SOCIETY: Our protocol can be applied in distributed systems where multiple servers exist[5]. For example, Microsoft active directory domain service (AD DS) is the foundation for distributed networks built on Windows server operating systems that use domain controllers. Based on our two-server PAKE protocol, we can split the user's password into two parts and store them, respectively, on the two AD DS domain controllers, which can then cooperate to authenticate the user. Even if one domain controller is compromised, the system can still work. In this way, we can achieve more secure AD DS.

WHETHER ANY PH.D. ENROLLED/PRODUCED OUT OF THE PROJECT: NO

NO. OF PUBLICATIONS OUT OF THE PROJECT: 1(paper is attached)

G. Karthika
(PRINCIPAL INVESTIGATOR)

2
(PRINCIPAL)
PRINCIPAL
Vignana Bharathi Institute of Technology
(Seal)
Aushapur(V), Ghatkesar(M), Medchal Dist-501 301



THESIS

Title of Minor Research Project: Cryptography Key
Exchange Authentication Using Two Servers PAKE

Principal Investigator: G.K.Karthika, Assistant
Professor ,Department of IT, Vignana Bharathi Institute
of Technology, Aushapur, Hyderabad.

UGC Reference No. F: MRP-6943/16 (SERO/UGC)

ABSTRACT

Password-authenticated key exchange (PAKE) is a technique where a client and a server share their passwords by authenticating each other mutually and establishing key through the reciprocation of messages. The context follows where the passwords needed to authenticate clients are being stored in a single unique server. Hence thereby disclosing those passwords stored if the server is collapsed due to attacks. In the current scenario the concept of two servers is introduced where the two servers cooperate with each other to authenticate a client and even if one of the servers is collapsed the attacker can still not become a client as the other server's information is not known. The solution provided is flavored in two: First is Symmetric in which a public key is generated and where two servers equally take part in authenticating a client. Second is Asymmetric in which a secret key is generated and where one server takes the help of other server to authenticate a client. This paper presents the symmetric solution for two servers PAKE. In addition to this a nonce is generated during authentication period that acts like a timer. If the timer is not expired after the period limit exceeds, the authentication process is carried out within the time limit to provide security and to replay attacks.

INDEX

1. Introduction	1
2. Literature Survey	7
3. Methodology	16
3.1 Algorithm	17
4. Results	20
5. Conclusion	22
Publications as part of UGC Project	23
References	24

1. INTRODUCTION

These days, passwords are regularly utilized by individuals during a sign in procedure that controls access to secured PC working frameworks, cell phones, satellite TV decoders, robotized teller machines, etc. APC client may require passwords for some reasons: signing in to PC accounts, recovering email from servers, getting to programs, databases, systems, web locales, and notwithstanding perusing the morning paper on the web. Prior secret key based confirmation frameworks transmitted cryptographic hash of the secret key over an open channel which makes the hash esteem open to an aggressor. At the point when this is done, and it is normal, the aggressor can work disconnected, quickly testing potential passwords against the genuine secret word's hash esteem. Studies have reliably demonstrated that an enormous portion of client picked passwords are promptly speculated consequently. For instance, as indicated by Bruce Schneier, looking at information from a 2006 phishing assault, 55 percent of MySpace passwords would-be crack able in 8 hours utilizing an industrially accessible Secret key Recovery Toolkit fit for testing 200,000 passwords every second in 2006. Ongoing exploration propels in secret

word based confirmation have permitted a customer and a server commonly to validate with a secret phrase and in the interim to build up a cryptographic key for secure interchanges after confirmation. All in all, current answers for password based confirmation pursue two models. The principal model, called PKI-based model, accept that the customer keeps the server's open key notwithstanding share a secret word with the server. In this setting, the customers can send the secret word to the server by open key encryption. Gongget al. were the first to exhibit this sort of verification conventions with heuristic impervious to disconnected lexicon assaults, and Halevi and Krawczyk were the first to give formal definitions and thorough evidences of security for PKI-based model. The subsequent model is called secret phrase just model. Bellovin and Merritt were the first to consider confirmation dependent on secret word just, and presented a set of alleged "scrambled key trade" conventions, where the secret phrase is utilized as a mystery key to scramble arbitrary numbers for key trade reason. Formal models of security for the secret phrase just verification were first given freely by Bellare et al. and Boyko et al. Katz et al. were the first to give a secret key as it we reconfirmation convention which is

both reasonable and provably secure under standard cryptographic presumption.

In view of the character based encryption method Yi et al. proposed a character based model where the customer needs to recollect the secret key as it were while the server keeps the secret key notwithstanding private keys identified with its character. In this setting, the customer can encode the secret key dependent on the personality of the server. This model is between the PKI-based and the secret key as it we remodels. A commonplace convention for secret key based validation expect a solitary server stores every one of the passwords important to validate customers. On the off chance that the server is undermined, due to, for instance, hacking, or introducing a "Trojan pony," or even insider assault, client passwords put away in the server are revealed. To address this issue, two-server secret phrase based confirmation conventions were presented, where two servers collaborate to confirm a customer based on secret key and in the event that one server is undermined, the assailant still can't claim to be the customer with the data from the traded off server.

We designed Two Server Password-authenticated key exchanges (PAKE) are where servers cooperate to authenticate a customer and if one server is

compromised, the attacker nonetheless can't pretend to be the consumer with the information from the compromised server. The present solutions for 2-server PAKE are either symmetric in the feel that peer servers equally contribute to the authentication or uneven within the feel that one server authenticates the customer with the assist of any other server. We're right here by means of looking to awareness on the symmetric answer for 2-server PAKE, in which the client can set up one of a kind cryptographic key with the 2 servers, respectively. Our protocol runs in parallel and is extra green than present symmetric -server PAKE protocol, or even more green than existing asymmetric two-server PAKE protocols in phrases of parallel computation. Similarly to that a nonce might be generated throughout the length of authentication and this may act as a timer. If the timer does no longer expire with in the period restrict, the authentication process might be achieved in the restriction which presents protection to replay assaults. A symmetric server PAKE protocol can run in parallel and establishes mystery session keys between the purchaser and servers, respectively. In case one of the servers shuts down due to the denial-of-service assault, some other server can continue to

provide services to authenticated clients. Safety analysis has proven that our protocol is secure in opposition to each passive and lively attack in case that one server is compromised. Performance evaluation has shown that our protocol is extra efficient than current symmetric and asymmetric -server PAKE protocols in terms of parallel computation.

Objective of Project

- The main objective of Two Server Password-authenticated key exchange protocol is to provide Security against passive and active attacks in case that one of the two servers is compromised.
- Performance analysis has shown that our protocol is more efficient than existing symmetric and asymmetric two-server PAKE protocols in terms of parallel computation and also it takes less communication rounds.
- In addition to the efficiency the authentication and key exchange should be completed within a time limit. Hence, the protocol is secure against replay attacks.

Scope:

Our protocol provides explicit authentication in the sense that each party knows that other parties have established their secret session keys correctly if the message authentication by the party succeeds. If the client C accepts the messages $M4$ and $M5$, the client C is confirmed that the servers $S1$ and $S2$ will compute their secret session keys with the client C correctly. If the server $S1$ accepts the message $M6$, the server $S1$ is confirmed that the client C has computed the same secret session key $SK1$, and the client C and the server $S2$ have established their secret session key correctly.

2. LITERATURE SURVEY

In general, current solutions for password based authentication follow two models. The first model, called PKI-based model, assumes that the client keeps the server's public key in addition to share a password with the server. In this setting, the client can send the password to the server by public key encryption.

The second model is called password-only model which considers authentication based on password only, and introduced a set of so-called encrypted key exchange protocols, where the password is used as a secret key to encrypt random numbers for key exchange purpose.

The other model is Identity-based model where the client needs to remember the password only while the server keeps the password in addition to private keys related to its identity. In this setting, the client can encrypt the password based on the identity of the server. This model is between the PKI-based and the password only models.

KEA is a Diffie-Hellman based key exchange protocol developed by NSA which provides mutual authentication for the parties. It became publicly available in 1998 and since then it was neither attacked nor proved to be secure.

KEA involves 2 parties, A and B, with respective secret keys a and b and public

keys g_a and g_b . We assume that parties know each other's registered public keys.

The main idea behind KEA+ is to incorporate parties' identities in the computation of a session key. Interestingly, this simple feature of the protocol turns out to be crucial in the security analysis and avoids the proof-of-possession requirement.

KEA+ is resistant to Unknown Key Share Attacks. The 2-pass KEA+ protocol is optimized for communication and has exactly the same communication as the original DiffieHellman protocol.

ElGamalEncryptionScheme:

Each user has a private key x Each user has three public keys: prime modulus p , generator g and public $Y = g^x \bmod p$

Security is based on the difficulty of DLP Secure key size > 1024bits (today even 2048bits) Elgamal is quite slow, it is used mainly for key authentication protocols.

2.1 For the study of password-based protocols for authenticated key exchange (AKE). We consider the scenario in which there are two entities|a client A and a server B|where A holds a password pw and B holds a key related to this. The parties would like to engage in a conversation at the end of which each holds a session key, sk , which is known to nobody but the two of them. There is present an active adversary A whose capabilities include enumerating, o-line, the words in a dictionary D, this dictionary being rather likely to include pw . In a protocol we deem "good" the adversary's chance to defeat protocol goals will depend on how much she interacts with protocol participants|it won't significantly depend on her o-line computing time.

2.2 Passwords are the most widespread means of user authentication.

► In existing solutions for password-based authentication, users' passwords are revealed if the server is compromised.

► The potential damage from server compromise can be mitigated if multiple servers are used. ► We propose and prove secure the first two-server protocol

for password-only authentication. ► Our protocol is efficient, using only a small constant factor more computation than existing schemes.

2.3 Taking advantage of the special structure of a federated enterprise, a new architecture comprising an external server and a central server was proposed. A user authentication and key exchange protocol using password that is geared to the architecture was presented. Attention was focused on resisting off-line dictionary attacks by the servers, a topic rarely considered in previous effort.

2.4 Two-server password authentication and key exchange system is secure against offline dictionary attacks by servers when they are controlled by adversaries. This is a password-only system in the sense that it requires no public key cryptosystem and, no PKI. It generalizes the basic two-server model to architecture of a single back-end server supporting multiple frontend servers and envisions interesting applications in federated enterprises. In authentication schema SMS integration API are used for two step verification like Gmail, as it provides the additional security to end user.

2.5 Passwords are the most common way to prove identity of user when accessing protected data, accounts and your computer itself (via User Accounts). The use of strong passwords is therefore essential in order to protect your security and identity. The best security in the world is useless if a malicious person has a legitimate user name and password. A password is a secret word or set or collection of characters used for user authentication to prove identity or access approval to gain access to a resource (example: an access code is a type of password), which should be kept secret from unauthorized person. Unfortunately, many security systems are designed such that security relies entirely on a secret password. Many researchers show that people pick easy to guess passwords. For example, an early study on password security found that over 15% of users picked passwords shorter or equal to three characters.

Recent research advances in password-based authentication have allowed a client and a server mutually to authenticate with a password and meanwhile to establish a cryptographic key for secure communications after authentication. The current solutions for password based authentication follow two strategies.

In first strategy, assumes that the client keeps the servers public key in addition to share a password with the server. The second strategy is called password-only strategy which introduces a set of so-called encrypted key exchange protocols, where the password is used as a secret key to encrypt random numbers for key exchange purpose.

2.6 The main goal of cryptography is to enable secure communication in a hostile environment. If two parties P_i and P_j want to safely communicate over a network occupied by an active adversary, usually P_i and P_j will want to ensure the privacy and authenticity of the data they send to each other. To this end they will encrypt and authenticate their transmissions. But before P_i and P_j want to use these tools they will need to have keys, without keys cryptography simply cannot get to the ground. Much research in modern cryptography has focused on how to use keys to provably achieve goals like encryption and signatures.

2.7 A natural solution in the setting under consideration is an encrypted challenge-response protocol. Roughly speaking, the server generates a public key, private key pair. The users are all informed of the public key. When a user

u attempts to log in, the server sends in the clear a challenge r to u , and u must reply with an encryption, under the server's public key, of u , r , and u 's secret password, denoted spw_u . The critical question in making such an approach work is the type of security that must be enjoyed by the cryptosystem. To see this, suppose the cryptosystem is malleable¹, and consider the case in which u , in response to a challenge r , responds with an encryption $c = E(\text{spw}_u; u; r)$. Then v , impersonating u and receiving a challenge r_0 , may be able to transform c to $c_0 = E(\text{spw}_u; u; r_0)$. This is trivial if encryption is bit-by-bit, so semantic security is clearly insufficient (because there exist semantically secure bit-by-bit encryption schemes, e.g. [13]). As this example shows, some nonmalleability is essential to implementing the encrypted challenge-response approach.

2.8 This problem is of growing importance as Internet-enabled computing devices become ever more prevalent and versatile. These devices now include among their ranks an abundant variety of mobile phones, personal digital assistants (PDAs), and game consoles, as well as laptop and desktop PCs. The availability of networks of computers to highly mobile user populations, as in

corporate environments, means that a single user may regularly employ many different points of remote access. The roaming user may additionally employ any of a number of different devices, not all of which necessarily possess the same software or configuration. While smartcards and similar key-storage devices offer a secured, harmonized approach to authentication for the roaming user, they lack an adequately developed supporting infrastructure in many computing environments. At present, for example, very few computing devices contain smartcard readers – particularly in the United States. Furthermore, many users find physical authentication tokens inconvenient. Another point militating against a critical reliance on hardware tokens is the common need to authenticate roaming users who have lost or forgotten their tokens, or whose tokens have malfunctioned. Today, this is usually achieved by asking users to provide answers to a set of “life” questions, i.e., questions regarding personal and private information. These observations stress that roaming users must be able to employ passwords or other short pieces of memorable information as a form of authentication. Indeed, short secrets like passwords and answers to life questions are the predominant form of authentication for most users today. They

are the focus of our work here. To ensure usability by a large user population, it is important that passwords be memorable. As a result, those used in practice are often highly vulnerable to brute-force guessing attacks [21]. Good credential-server designs must therefore permit secure authentication assuming a weak key (password) on the part of the user.

3. METHODOLOGY

In our system, there exist two servers S1 and S2 and a group of clients. The two servers cooperate to authenticate clients and provide services to authenticated clients. Prior to authentication, each client C chooses a password pw_C and to S1 and S2, respective, through different secure channels during the client registration. After that, the client remembers the password only, and the two servers keep the password authentication information. Like all existing solutions generates the password authentication information $Auth_C^{(1)}$ and $Auth_C^{(2)}$ for S1 and S2, respectively, such that nobody can determine the password pw_C from $Auth_C^{(1)}$ or $Auth_C^{(2)}$ unless S1 and S2 collude. The client sends $Auth_C^{(1)}$ and $Auth_C^{(2)}$ for two-server PAKE, we assume the two servers never collude to reveal the password of the client. When the two servers cooperate to authenticate a client C, we assume that the client C can broadcast a message to both of S1 and S2 simultaneously, but stress that we do not assume a broadcast channel and, in particular, an attacker can deliver different messages to the two servers or refuse to deliver a message to a server. In our protocol, the

client and the two servers communicate through a public channel which may be eavesdropped, delayed, replayed, and even tampered by an attacker. Our protocol is symmetric if two peer servers equally contribute to the authentication in terms of computation and communication.

3.1 Algorithm :

ElGamal Encryption:

In cryptography, the ElGamal encryption framework is a lopsided key encryption calculation for open key cryptography. The ElGamal encryption plan was created by ElGamalin 1985 based on Diffie-Hellman key trade convention.

It comprises of key age, encryption, and unscrambling algorithms as follows:

Key Generation: On information a security parameter k , it distributes a cyclic gathering G of huge prime request q with a generator g . At that point it picks a decoding key x arbitrarily from Z_q and processes an encryption key $y = g^x$.

Encryption: On inputs a message $m \in G$ and the encryption key y , it chooses an integer r randomly from Z_q and outputs a ciphertext

$$C = \mathcal{E}(m, y) = (A, B) = (g^r, m \cdot y^r).$$

Decryption: On data sources a ciphertext (A,B) , and the decoding key x , it yields the plaintext $m=D(C,x)=B/A^x$.

ElGamal encryption plan is a probabilistic encryption plot. On the off chance that encoding a similar message with ElGamal encryption conspires a few times, it will, when all is said in done, yield diverse ciphertexts. Tsionis and Yung demonstrated ElGamal encryption plan to be semantically secure under the DDH supposition.

ElGamal Encryption Scheme: The ElGamal encryption scheme was invented by ElGamal in 1985 on the basis of Diffie-Hellman key exchange protocol. It consists of key generation, encryption, and decryption algorithms. ElGamal encryption scheme is a probabilistic encryption scheme. If encrypting the same message with ElGamal encryption scheme several times, it will, in general, yield different ciphertexts. Encryption Algorithm works as follows:

Key Generation: Participant A generates the public/private key pair

- a. Generate large prime p and generator g of the multiplicative Group Z^*_p of the integers modulo p .
- b. Select a random integer a , $1 \leq a \leq p - 2$, and compute $ga \bmod p$.

c. A's Public key is (p, g, g^a) . A's Private key is a .

Encryption: Participant B encrypts a message m to A

a. Obtain A's authentic public key (p, g, g^a) .

b. Represent the message as integer's m in the range $\{0, 1, 2, \dots, p-1\}$

c. Select a random integer k , $1 \leq k \leq p - 2$.

d. Compute $\gamma = g^k \bmod p$ and $\delta = m * (g^a)^k$

e. Send cipher text $c = (\gamma, \delta)$ to A.

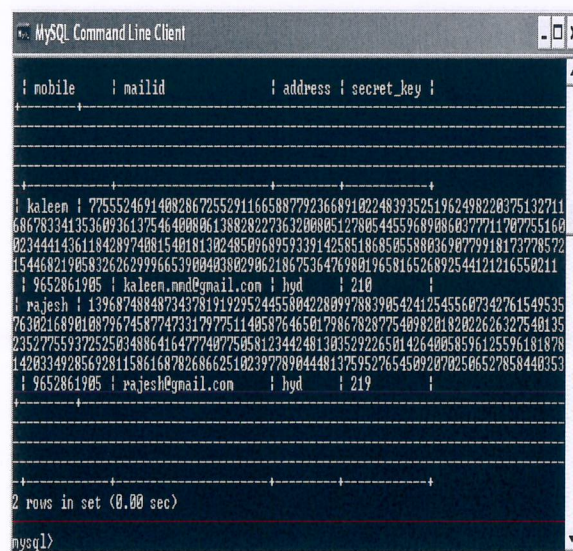
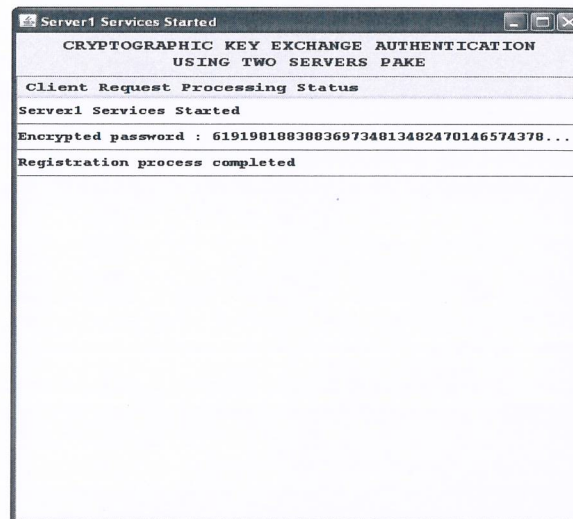
Decryption: Participant A receives encrypted message m from B

a. Use private key a to compute $(\gamma^{p-1-a}) \bmod p$.

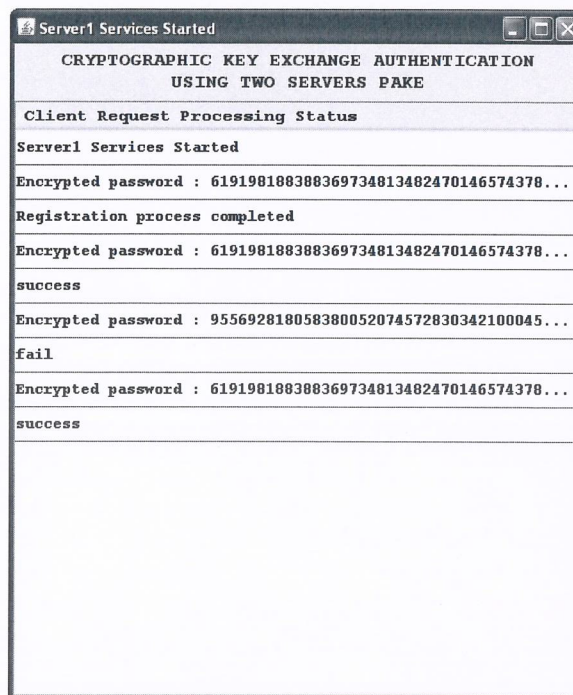
b. Recover m by computing $(\gamma^{-a}) * \delta \bmod p$.

4. RESULTS

we examine the presentation of our convention what's more, contrast our convention and existing conventions for two server secret phrase just validation and key trade. In database also we can see password save in encrypted format.



Now click on login button to authenticate user with two servers. Then in that screen, we can see user login successfully by using two servers. Now close black console of one server and then still we can login. This means even more server down then second server can able to login user or provide services to the user. See below server screen for password.



CONCLUSION

The concept outlined in this work is as the users can be authenticated using two servers in such a way that initially the password of a user will be divided into two parts, and subsequently the secret key is generated for each part. The password, which had to split into two parts, will be encrypted using Elgamal Encryption. Each encrypted part, and its associated key will be sent to the two servers. Therefore, each server contains its own key, if an intruder intelligently makes one server to be compromised, even in that case too, the second server will not allow the intruder to log into the system until and unless the appropriate credentials are entered.

Acknowledgment

I gratefully acknowledge the computational facility provided in the college under SERO -UGC MINOR RESEARCH PROJECT MRP ID: MRP UGC6943/16 with proposal number [1377] titled “Cryptographic Key Exchange Using Two Servers PAKE” with which helped me to carry out the work. I thank the management of Vignana Bharathi Institute of Technology for their support and kind encouragement.

Publications as part of UGC Project

Published a research paper “Cryptographic Key Exchange Authentication using Two Servers PAKE” International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8 Issue-6S, August 2019

References

- [1]. M. Bellare, D. Pointcheval, P. Rogaway, “Authenticated Key Exchange Secure Against Dictionary Attacks, *Advances in Cryptology*” —Eurocrypt ’00, pp. 139–155, Springer-Verlag, 2000.
- [2]. J. Katz, P. MacKenzie, G. Taban, and V. Gligor, “Two-Server Password-Only Authenticated Key Exchange,” *Proc. Applied Cryptography and Network Security (ACNS ’05)*, pp. 1-16, 2005.
- [3]. Y. Yang, F. Bao, and R.H. Deng, “A New Architecture for Authentication and Key Exchange Using Password for Federated Enterprise,” *Proc. 20th ’05*, pp. 95-111, 2005.
- [4]. H. Jin, D.S. Wong, and Y. Xu, “An Efficient Password-Only Two-Server Authenticated Key Exchange System,” *Proc. Ninth Int’ Conf. Information and Comm. Security (ICICS ’07)*, pp. 44-56, 2007.
- [5]. D. Jablon, “Password Authentication Using Multiple Servers,” *Proc. Conf. Topics in Cryptology: The Cryptographer’s Track at RSA (RSA-CT ’01)*, pp. 344-360, 2001.
- [6]. Bellare, M., Rogaway, P.: Provably-Secure Session Key Distribution: the Three Party Case. In: *27th ACM Symposium on Theory of Computing (STOC)*, pp. 57–66. ACM, New York (1995).
- [7]. Boyarsky, M.: Public-Key Cryptography and Password Protocols: The Multi-User Case. In: *7th Ann. Conf. on Computer and Comm. Security*, pp. 63–72. ACM, New York (1999).
- [8]. Brainard, J., Juels, A., Kaliski, B., Szydlo, M: Nightingale: A New Two-Server Approach for Authentication with Short Secrets. In: *12th USENIX Security Symp.*, pp. 201–213 (2003).

- [9]. Brainard, A. Juels, B. Kaliski, M. Szydło, Nightingale: A new two-server approach for authentication with short secrets, in: 12th USENIX SecuritySymp., 2003, pp. 201–213.
- [10]. R. Canetti, O. Goldreich, S. Halevi, The random oracle methodology, revisited, J. ACM 51 (4) (2004) 557–594.
- [11]. R. Canetti, S. Halevi, J. Katz, Y. Lindell, P. MacKenzie, Universally-composable password authenticated key exchange, in: Adv. in Cryptology –Eurocrypt2005, in: Lecture Notes in Comput. Sci., vol. 3494, Springer-Verlag, 2005, pp. 404–421.
- [12]. R. Cramer, Modular design of secure yet practical cryptographic protocols, PhD thesis, CWI and University of Amsterdam, 1996.
- [13]. R. Cramer, I. Damgård, B. Schoenmakers, and Proofs of partial knowledge and simplified design of witness hiding protocols, in: Adv. in Cryptology – Crypto1994, in: Lecture Notes in Comput. Sci., vol. 839, Springer-Verlag, 1994, pp. 174–187.
- [14]. R. Cramer, V. Shoup, Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack, SIAM J. Comput. 33 (1) (2003) 167–226.
- [15]. W. Diffie, M. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory 22 (6) (1976) 644–654.
- [16]. M. Di Raimondo, R. Gennaro, Provably secure threshold password-authenticated key exchange, J. Comput. System Sci. 72 (6) (2006) 978–1001.
- [17]. T. El Gamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. Inform. Theory 31 (1985) 469–472.
- [18]. W. Ford, B.S. Kaliski, Server-assisted generation of a strong secret from a password, in: Proc. 5th IEEE Intl. Workshop on Enterprise Security, 2000.

- [19]. R. Gennaro, Y. Lindell, A framework for password-based authenticated key exchange, *ACM Trans. Inf. Syst. Secur.* 9 (2) (2006) 181–234.
- [20]. O. Goldreich, Y. Lindell, Session-key generation using human passwords only, *J. Cryptology* 19 (3) (2006) 241–340, preliminary version in *Crypto* 2001.
- [21]. L. Gong, T.M.A. Lomas, R.M. Needham, J.H. Saltzer, Protecting poorly-chosen secrets from guessing attacks, *IEEE J. Sel. Areas Commun.* 11 (5) (1993) 648–656.
- [22]. S. Halevi, H. Krawczyk, Public-key cryptography and password protocols, *ACM Trans. Inf. Syst. Secur.* 2 (3) (1999) 230–268.
- [23]. D. Jablon, Strong password-only authenticated key exchange, *ACM Comput. Commun. Rev.* 26 (5) (1996) 5–20.
- [24]. D. Jablon, Password authentication using multiple servers, in: *RSA Cryptographers' Track 2001*, in: *Lecture Notes in Comput. Sci.*, vol. 2020, Springer-Verlag, 2001, pp. 344–360.
- [25]. S. Jiang, G. Gong, Password based key exchange with mutual authentication, *Workshop on Selected Areas of Cryptography (SAC)*, 2004

Cryptographic Key Exchange Authentication using Two Servers PAKE

G.K. Karthika, Raju Dara, Yamini Devi. N

Abstract— The key trade procedure is well thought-out significant fractions of cryptographic method towards defend protected end-to-end communications. All existing techniques need two servers to be active to authenticate but this technique can authenticate even one server is up and other server is down due to attack as active server authenticate user by taking his parts. In this paper, design an idea Password-authenticated key exchange (PAKE) method to verify clients by utilizing two servers, first client secret phrase will be splitted into two sections and afterward mystery key will be produced for each part and after that by utilizing key and splitted secret phrase will be encoded utilizing ElGamal Encryption. Each encoded part and key will be send to every server. Every server will have its very own key and in the event that aggressor traded off one server, at that point he won't ready to login till he got client information of second server, by utilizing this strategy no assailant can bargain the two servers.

Keywords: Cryptography, ElGamal Encryption, Password Authenticated Key Exchange (PAKE).

I. INTRODUCTION

These days, code word are regularly utilized by individuals during a sign in procedure so as to have power over way in to verified PC running system, phones, satellite TV decoders, robotized teller machinery, etc. APC client possibly will necessitate code word intended for some reasons: signing within towards PC explanation, recovering email from servers, attainment on the way to programs, record, scheme, web locales, along with in spite of pay particular attention on the web. Prior secret key based confirmation frameworks transmitted cryptographic hash of the secret key more an open conduit which construct the confusion esteem open on the way to an aggressor. At the point while this be completed, as well as it be normal, the aggressor be able to effort disconnected, quickly testing potential secret word alongside the genuine secret word's confusion esteem. Learn contain reliably demonstrated so as to an enormous portion of client picked passwords are promptly speculated consequently. For instance, as indicated by Bruce Schneier, looking at information from a 2006 phishing assault, 55 percent of MySpace code words prospective break capable within 8 hours utilizing an industrially accessible Secret key Recovery Toolkit fit for testing 200,000 passwords every second in 2006. Ongoing exploration propels in secret word based

confirmation have permitted a customer as well as a attendant commonly towards validate by way of a secret phrase along with in the interim on the way to build awake a cryptographic input meant for safe interchanges subsequent to confirmation. All within all, present answers designed for code word support confirmation pursue two representations. The principal representation, known as PKI-based form, accept so as to the customer maintains the server open key notwithstanding distributes a secret word through the server. Within these surroundings, the customers know how to send the secret word towards the server next to open key encryption. Gong et al. be the primary towards exhibit this sort of verification conventions among heuristic impervious near disconnected lexicon assaults, Halevi as well as Krawczyk be the initial towards give proper description also thorough evidences of safety meant for PKI-based design. The subsequent design was known as secret phrase just method. Bellare along with Merritt be the primary in the direction of believe confirmation dependent lying on secret word just, moreover presented a position of alleged "scrambled key in trade" conventions, anywhere the secret phrase be utilized because a mystery key in to scramble arbitrary information meant for key in trade reason. proper form of safety designed for the secret phrase just verification be initial specified freely through Bellare et al. as well as Boyko et al. Katz et al. be the first towards provide secret key as it we reconfirmation convention which is both reasonable along with verifiably safe beneath criterion cryptographic presumption. In view of the character based encryption method Yi et al. proposed a character pedestal form anywhere the customer wants towards recollect the secret key as it were while the server keeps secret key notwithstanding private keys identified with its character. Within this background, the customer be able to encode the secret key dependent resting on the personality of the attendant. This reproduction be stuck between the PKI-based as well as the secret key as it we remodels. A commonplace convention for secret key based validation expect a solitary server stores every one of the passwords important to validate customers. On the off chance that the server be undermined, owing towards, designed for instance, slash, otherwise introducing a "Trojan pony," or else still within assault, client secret words put away inside the server be revealed. in the direction of tackle this subject, two-server secret phrase pedestal confirmation conventions were presented, where two servers collaborate to confirm a customer based on secret key and in the event that one server is undermined, the assailant still

Revised Version Manuscript Received on August 14, 2019.

Ms. G.K. Karthika, Asst. Professor, Dept., of Information Technology, Vignana Bharathi Institute of Technology, Hyderabad, Telangana, India.
(E-Mail: kalpeesri@gmail.com)

Dr. Raju Dara Professor, Dept., of Computer Science & Engineering, Vignana Bharathi Institute of Technology, Hyderabad, Telangana, India.
(E-Mail: rajurdara@gmail.com)

Ms. Yamini Devi. N Dept., of Computer Science & Engineering, Vignana Bharathi Institute of Technology, Hyderabad, Telangana, India.
(E-Mail: kalpeesri@gmail.com)


```

MySQL Command Line Client

+-----+-----+-----+-----+
| nobile | nailed | address | secret_key |
+-----+-----+-----+-----+

1 | kileen | 77555246914082867255291166588779236891022483935251962498220375132711
68678334135360936137546400806138828227363200805127805445596890860377211707755160
02344414361184289740815401813024850968959339142585186850558803690779918173778572
1544682190583262629996653900403802906218675364769801965816526892544121216550211
1 | 9652861905 | kileen.mnd@gmail.com | hyd | 210
1 | rajesh | 139687488487343781919295244558042280997883905424125455607342761549535
76302168901087967458774733179775114058764650179867828775409820182022626327540135
23527755937252503488641647774077506812344248130352922650142640058596125596181878
1420334928569281158616878268662510239778904481375952765450920702506527858440353
1 | 9652861905 | rajesh@gmail.com | hyd | 219

2 rows in set (0.00 sec)

mysql>

```

Now click on login button to authenticate user with two servers. Then in that screen, we can see user login successfully by using two servers. Now close black console of one server along with then still we can login. This means even more server down then second server can able to login user or provide services to the user. See below server screen for password.



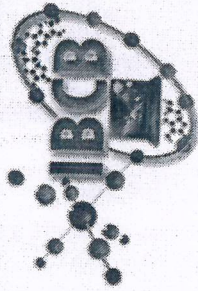
IV. CONCLUSION

In this paper, we planned a concept to authenticate users by using two servers, first user password will be splitted into two parts along with then secret key will be generated for each part along with then by using key along with splitted password will be encrypted using Elgamal Encryption. Each encrypted part along with key will be send to each server. Each server will have its own key along with if attacker compromised one server then he won't able to login till he got user data of second server, by using this technique no attacker can compromise both servers.

REFERENCES

1. Alix. "Predictive estimation of protein linear epitopes by using the program PEOPLE". Vaccine, 18:311–4, 1999.
2. Argos, P., Rossmann, M.G., Grau, U.M., Zuber, H., Frand, G., & Tratschin, J.D. (1979) Biochemistry **18**,

- 5698-5703
3. Atassi, M. Z. & Lee, C. L. (1978) Biochemistry **171**, 429-434.
4. Atassi, M. Z. (1975) Immunochemistry **12**, 423-438.
5. Atsushi Ikai(1980)..., "Thermostability and Aliphatic Index of Globular proteins"... Biochem. **88**, 1895-1898 (1980)
6. B. Peters, J. Sidney, P. Bourne, H. Bui, S. Buus, G. Doh, W. Fleri, M. Kronenberg, R. Kubo, O. Lund, et al. "The Immune Epitope Database and Analysis Resource: From Vision to Blueprint". PLoS Biology, **3**:e91, 2005.
7. Bachmair.A., Finley.D. and Varshavsky.A. (1986) Science, **234**, 179-186.
8. Baranyi L, Campbell W, Ohshima K, Fujimoto S, Boros M, Okada H. "The antisense homology box. a new motif within proteins that encodes biologically active peptides". Nat. Med 1995, **1**, pp. 894-901.
9. Barlow,D.J., Edwards, M.S., and Thornton,J.M., 1986 "Continuous and discontinuous protein antigenic determinants". Nature, Vol 322, pp747-748.
10. Berchanski A, Shapira B, Eisenstein M. "Hydrophobic complementarity in protein protein docking". Proteins 2004, **56**, pp. 130-142.
11. Chen. J, H. Liu, J. Yang, and K. Chou." Prediction of linear B-cell epitopes using amino acid pair antigenicity scale". Amino Acids, **33**:423–428, 2007.
12. Chou PY, Fasman GD. 1974. "Conformational parameters for amino acids in helical, &sheet and random coil regions calculated from proteins". Biochemistry **13**:211-223.
13. Clements JD, Martin RE. "Identification of novel membrane proteins by searching for patterns in hydropathy profiles". Eur. J. Biochem 2002, **269**, pp. 2101-2107.
14. Creighton.T.E. (1988) BioEssays, **8**, 57-63.
15. Curr "...Design of synthetic peptides for diagnostics", Protein Pept Sci, **4**(4):253-260, 2003.
16. D. Flower. "Immunoinformatics: "Predicting immunogenicity in silico". Quantum distributor, 1st edition, 2007.
17. T. El Gamal, A public key cryptosystem along with a signature scheme based on discrete logarithms, IEEE Trans. Inform. Theory **31** (1985) 469–472.
18. W. Ford, B.S. Kaliski, Server-assisted generation of a strong secret from a password, in: Proc. 5th IEEE Intl. Workshop on Enterprise Security, 2000.
19. R. Gennaro, Y. Lindell, A framework for password-based authenticated key exchange, ACM Trans. Inf. Syst. Secur. **9** (2) (2006) 181–234.
20. O. Goldreich, Y. Lindell, Session-key generation using human passwords only, J. Cryptology **19** (3) (2006) 241–340, preliminary version in Crypto 2001.
21. L. Gong, T.M.A. Lomas, R.M. Needham, J.H. Saltzer, Protecting poorly-chosen secrets from guessing attacks, IEEE J. Sel. Areas Commun. **11** (5) (1993)648–656.
22. S. Halevi, H. Krawczyk, Public-key cryptography along with password protocols, ACM Trans. Inf. Syst. Secur. **2** (3) (1999) 230–268.
23. D. Jablon, Strong password-only authenticated key exchange, ACM Comput. Commun. Rev. **26** (5) (1996) 5–20.
24. D. Jablon, Password authentication using multiple servers, in: RSA Cryptographers' Track 2001, in: Lecture Notes in Comput. Sci., vol. 2020, Springer-Verlag, 2001, pp. 344–360.



6th International Conference on



ADVANCED LOGICAL LEARNING AND
ANALYTICAL MINING (ALLAM) IN COGNITIVE SCIENCE, 28th December 2019

Organised by

Institute of Bioinformatics and Computational Biology (IBCB), Visakhapatnam
(Recognized as SIRO by Department of Science & Technology, Government of India)

Certificate

This is to certify that Dr/Mr/Mrs/Miss *S.K. KARTHIKA*
has presented a paper titled *Cryptographic Key Exchange Authentication*
Using Two Servers Pake..... at the International conference
on Advanced Logical Learning and Analytical Mining (ALLAM) in Cognitive Science during 28th December
2019, held at Andhra University, Visakhapatnam, A.P., India.


Dr K. Nageswar Rao
Convener,


Prof. Allam Appa Rao
General Chair,