PASSWORD AUTHENTICATED KEY EXCHANGE PROTOCOL WITH TWO SERVER BY IBE IN DATA ANALYTICS.

Priyadharshini.A,Logammbal.R,Anandhi .S

Vivekanandha college of engineering for women (Autonomous)

Abstract— **Communication between two parties needs security, so we introduce the protocol called PAKE (password authenticated key exchange), here client divide its password into two shares that is stored in 2S (two servers), these 2 server communicate or coordinate to each other without knowing the password of client because if any server get compromised by an opponent, password of client have to be remain secure, we present a two server based PAKE protocol on the basis of IBE (Identity Based Encryption) by using this we achieve implicit authentication. So far two party PAKE and IBE provable secure without random oracles compare with katz et al's 2S PAKE, our IBE 2S PAKE protocol can save computation in each server**

Index Term-PAKE,IBE,2Server,Ant optimization

I. INTRODUCTION

The encrypted key by follows protocol implementation specially used for transmission of secure data between two ends.The authenticated key in protocol needed for communication between two system procedure. In previous model, the secret key is preserved between the two parties for data transmission. Based on the model during communication the strongly connected data need extra preservation ,so one way of communication private key-encryption/decryption used for signing between one end to another end .As for another way public key is signing for Encryption/Decryption between two parties. The Key representation is difficult to maintain and using method involves in encryption is difficult to implement. In practice, the keys involves in authenticated purpose for secret communication is very important for further implementation.Another way of encrypted key can protected in personnal device,by password against hackers hacking the secret key.This may leak of password to third party.So "human –rememberable"keeping password in memory only way to avoid the hacking.

Bellovin and Merritt [3] were use the password-based authenticated key exchange (PAKE) protocol,through cryptographic key encryption secure communication is transformed between two ends for secret communication to reduce the possibility of hacking .

. A PAKE protocol haspossibility to work in on-line and off-linegroupingdictionaryattacks.

Inanoff-linegroupingdictionaryattack.Among them preferable to online grouping attacks the third party can login number of times to break the password and tries to collect all details of particular project.In offline grouping dictionary attacks it try to match the collected password with current running module password with number of possible attempts. To break the password the online grouping dictionary attack preferable chosen by hackers ,adversary to stop the attack threshold level can be fixed with automatically.

The number of attempt reached threshold level means the automatic message generated to stop the further processing. This method can efficiently increase by saving the password in two server to stop the hackers to break the password. Preferably offline grouping attack only less preferable to hackers try to break the password.

II ARCHITECTURE DESIGN

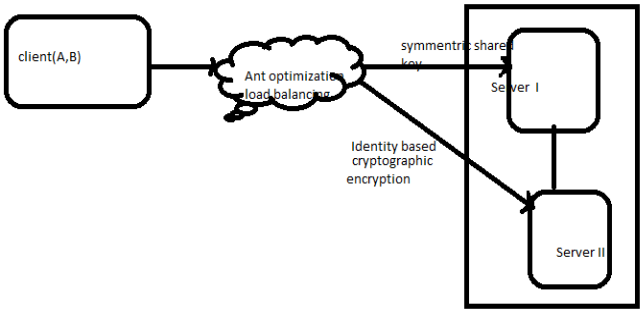


Fig1.1 SYSTEM ARCHITECTURE

III RELATED WORK

ID-based PAKE: ID-based PAKE protocols were proposed by Yi et al. [2],encrypted key save the private password in the identical server,their respected client need to remember the password in identical server. Promisely client

needs to remember a password in addition to the identity of the server, where as the server keeps the password in addition to a private key related to its identity. ID-based PAKE and PKI-based PAKE can apply the encryption/decryption communication protocol using only password generation method during transmission.The way of using protocol transmission using password generation by two methods (i) single-server and (ii)Multi-server.In the single-server setting, the authentication of all password generation conditionally satisfying after the client then only allow to store in single server. Hackers can compromise the single server easily and break the password and started to take their needed things . If the server is compromised, may also one of the reason that they are true kerberos for secure communication.For example hackers invade the system and by using number of ways to break the username and password against their respected identical server.To address this problem, the multi-server setting for PAKE was first suggested in [4], the particular identical password of the client can accumulated in multi servers by following PAKE protocols. PAKE protocols in the multi-server setting can be classified into two categories,(i) Threshold PAKE,(ii) Two Server PAKE

A. **Security challenges for the public cloud**

Cloud computing rule the communication part of world in network administration.Online communication is the most exciting work participated major role in cloud computing. The major concern of cloud computing need privacy and security in secure communication .To adopt the cloud computing concept by adopting various methods and challenges are outlined and its overcomes methods from its threats can adopt by using optimization. Here the Ant colony optimization can implement with security and privacy issues using PAKE protocol in two server can give trust worthy cryptographic communication.

B. **Public key encryption with Ant optimization**

D. Boneh, G. Di Crescenzo, et al here discuss about searching particular data among all data streams through encrypted data communication. Consider one source end user sends email by encryption /decryption to another end user Alice encrypted under Alice's public key. An email gateway allows the server

to communicate and check whether the data contains keyword “immediate” means it provide the way of communication fastly. The another end Alice able collect the data without any loss and communicate quickly by Ant Optimization technique. Eventhough the word “Immediate” indicates quick transmission to Alice Ant optimization techniques provides base for quick retrieval data without revealing data to third party.After approval of Alice, on the other hand then only can able to decrypt and accept the message. By using the method of “Public Key Encryption with Search keyword” gateway able to reveal the data to Alice without identifies the content of anything else. The “Immediate” keyword helps with optimization techniques for easy communication for transferring data to another end without revealing the particular content of data.The Public key Encryption mechanism also follows some keyword which helps to provide secure communication.

C. **Data integrity Preserving Keyword on remote cloud**

We consider the following problem: Optimization helps in cloud computing for proper utilization and sharing of resource.It will be very convenient method performs along with Encryption/Decryption method for resource utilization with cryptographic communication.

Consider in problem a one trusted user X wants to retrieve only needed collected data from total transmission of data in secure communication.All the group of message can encrypted in single signature and that can transmitted to another end under the proper resource utilization in single public cryptographic key .For Example one user ,during travelling time he needed already saved email which was already encrypted in group formature for their integrity and security.Particularly he needs one old message and after retrieving that mail for their further processing,which was undergoes some critical operation without comprising security .That same message should again transmitted and save in encrypted form added to already present message.

This was very difficult to handle that condition, because identification of identity server without comprising security and should maintain data integrity some wants to store his files in an encrypted form on a remote file server S.

III.PROPOSED METHODOLOGY.

In this paper, we propose a new method based on new algorithm **ID2S PAKE** protocols insisted on two way identity-based signature scheme (TWIBS).Based on the method optimized data can ready to transfer between two ends.To ensure the safety purpose encryption key cryptography method can apply over **ID2S PAKE** protocols for more safety purpose. The basic idea of the proposed method is applying **ID2S PAKE** protocols on password during encryption.The strong password can split into two equal parts and store in service server.The strong entity data transmission can carry out by splitting password and saved into two respected server.Each server maintain separate private key for signing purpose for each authentication.In Key cryptography each server compromise its client by public key for encryption addition with identity-based signature on it. The signature can be verified by the client on the basis of the identity of the server. After the complete verification, the client submits to the server one share of the

password encrypted with the public key of the server.

On second way of communication decryption keys follow by both servers can derive the same one-time password.At same time both server should derive the same one-time password.Through **ID2S PAKE protocol** the two server can authenticate to each other in complete secure manner.The Katz et al.'s protocol is password-only, each client needs to remember their respected password for further communication.It may also composed of variety of public and private key model encryption. Our proposed protocols are identity based signature method is follows between client and each server.Client needs to remember the password,which should comparable should satisfy their respected identical server.The cryptography encryption involves identical based signature contain common public parameters,which includes the masterpublic key.The private key based signature also applicable on ID2S PAKE protocols related to his identity, by sharing the password.**Ant optimization** supports working with secure cryptographic encryption key exchange in addition with secure identity based PAKE protocol. By using optimization techniques it improve the efficiency of working method of PAKE protocol.

Advantages:

I) It provides a two server authenticated cryptographic key-exchange protocol in secure communication.

II) It prove its flexibility against offline grouping dictionary attacks and online grouping dictionary attacks when passwords are used

III) Ant Optimization well facilitated in cryptographic key exchange.

IV)Proper resource utilization and load balancing is followed in secure communication.

IV DESIGNING

A.Input Design

The system is mainly linked with secure information with invoking user. It will be more supportive to preserve data and increasing its efficiency for further data preparation.All needed steps are utilized for further processing to overcome from the error.The commited resources can also inspect by their respected client before password splitting into two server.The needed resources only processed in secure communication with the help of Ant optimization.The resources can accessed directly in cloud computing.This will be very useful to avoid wastage of extra resources and perfect load balanced is followed in cryptographic key exchange. The design of input focuses on controlling the limit accessing of resources, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The architecture of input design is fully based on secure and data integrity.The concept of Ant optimization is well utilized for proper resource utilization and equalize the load balancing in the distributed environment.Ant optimization gives most previlage use for data communication in distributed environment.It mainly concern with

1) How much amount of data should be given as input?

2) Inwhich order data are arranged for secure communication?

3)What type of identity based cryptography is used to guide for secure communication.

B.WorkFlowDesign

.Input Design is the process of large amount of data can be transmitted using Identity based signature cryptography method.It will suitable for secure communication and prevent third party to invade the current processing data.The Two splitting password concept in their identical server denotes its its identity in well utilized of resource amount.This design is mainly processed to avoid errors in the data and mention the correct direction to user for getting correct information from the computerized server.

2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3.When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

c. Output Design

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2.Select methods for presenting information.
3.Create document, report, or other formats that contain information produced by the system.
The output form of an information system should accomplish one or more of the following objectives.Convey information about past activities, current status or projections of theFuture.Signal important events, opportunities, problems, or warnings.Trigger an action.Confirm an action.

V IMPLEMENTATION & RESULT

User:

The user, who can be an individual or an organization originally storing their data in two server accessing the data.

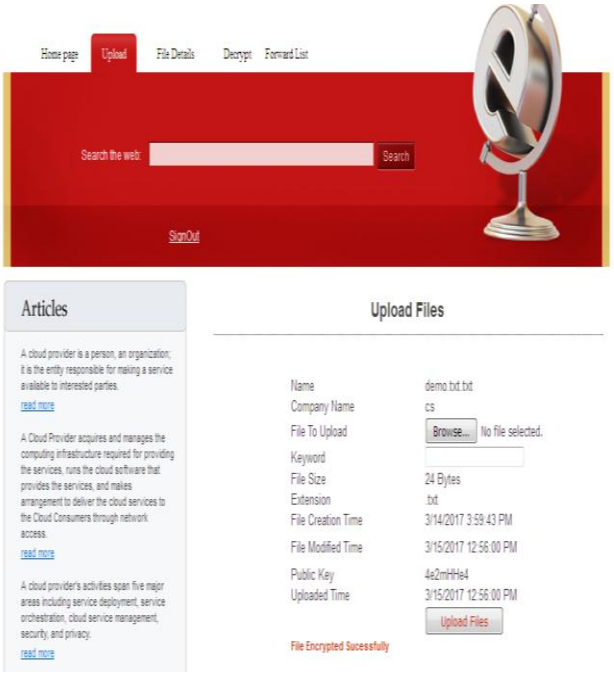


FIG.2. User profile

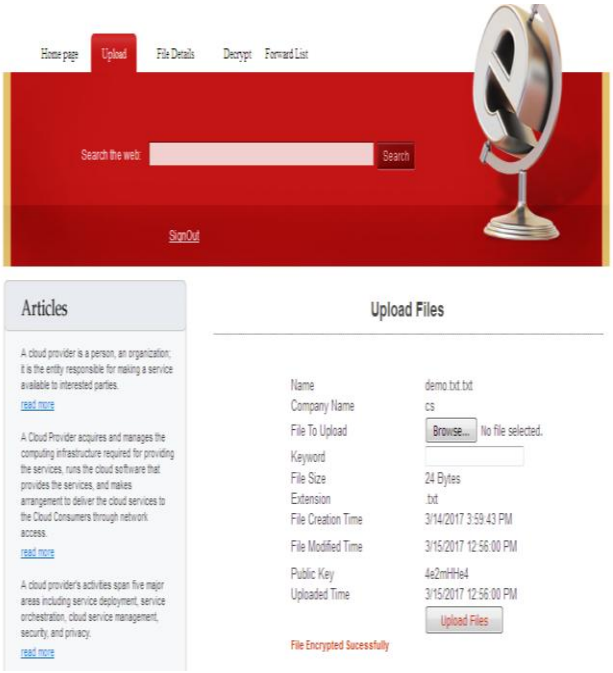


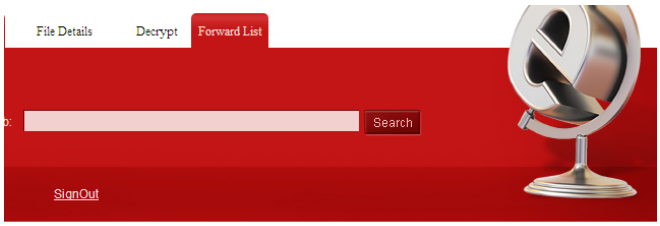
Fig.3.user information uploaded in server

Server:

After receiving the query from the receiver, the front server pre-processes the trapdoor and all the PAKE ciphertexts using its private key, and then sends some internal testing-states to the back server with the corresponding trapdoor and PAKE ciphertexts hidden.

Back Server:

In this module, the back server can then decide which documents are queried by the receiver using its private key and the received internal testing-states from the front server.
Decryption.
Uploaded files can be decrypted my using protocol IBE



Forward List

Sender	Receiver	Sending_Time	Sending_File	Key_Word
kad	select	3/14/2017 4:34:20 PM	demo.txt.txt	
kad	van	3/15/2017 11:22:41 AM	demo.txt.txt	
kad	daya	3/15/2017 1:00:06 PM	demo.txt.txt	

File forwarding

In thisfig uploaded files can be forwarded to the valid user

File Forwarding

Forward To daya

Users Public key DgeAbec1

Name	Company Name	File Name	File Size	Extension	Creation Time	Modified Time	Encrypted Time	KeyWord	
kad	cs	demo.txt.txt	24 Bytes	.txt	3/14/2017 3:59:43 PM	3/14/2017 4:34:02 PM	3/14/2017 4:34:03 PM		View File
kad	cs	demo.txt.txt	24 Bytes	.txt	3/14/2017 3:59:43 PM	3/15/2017 11:26:57 AM	3/15/2017 11:26:57 AM		View File
kad	cs	demo2.txt.txt	20 Bytes	.txt	3/14/2017 4:08:04 PM	3/15/2017 11:32:21 AM	3/15/2017 11:32:21 AM		View File
kad	cs	demo.txt.txt	24 Bytes	.txt	3/14/2017 3:59:43 PM	3/15/2017 12:56:00 PM	3/15/2017 12:56:00 PM		View File

IV CONCLUSION AND FUTURE ENHANCEMENT

In this paper we present two efficient compilers to transformany two-party PAKE protocol to an ID2S PAKE protocolwith identity-based cryptography. In addition, we have provided a rigorous proof of security for our compilerswithout random oracle. Our compilers are in particular suitablefor the applications of password-based authenticationwhere an identity-based system has already established.Our future work is to construct an identity-based multipleserverPAKE protocol with any two-party PAKE protocol.

REFERENCES

[1] S. M. Bellovin and M. Merritt. Encrypted key exchange: Passwordbased protocol secure against dictionary attack. In Proc. 1992 IEEE Symposium on Research in Security and Privacy, pages 72-84, 1992.

[2] W. Ford and B. S. Kaliski. Server-assisted generation of a strongfrom a password. In Proc. 5th IEEE Intl. Workshop onEnterprise Security, 2000.

[3] X. Yi, R. Tso and E. Okamoto. ID-based group passwordauthenticated key exchange. In Proc. IWSEC'09, pages 192-211, 2009.

[4] X. Yi, R. Tso and E. Okamoto. Identity-based passwordauthenticated key exchange for client/server model. In SECRYPT' 12, pages 45-54, 2012.

[5] B. Waters. Efficient identity-based encryption without randomoracles. In Proc. Eurocrypt'05, pages 114-127, 2005.

[6] Y. Yang, F. Bao, R. H. Deng. A new architecture for authenticationand key exchange using password for federated enterprise. InProc. SEC'05, pages 95-111, 2005.

[7] Y. Yang, R. H. Deng, and F. Bao. A practical password-basedtwo-server authentication and key exchange system. IEEE Trans.Dependable and Secure Computing, 3(2), 105-114, 2006.

[8] Y. Yang, R. H. Deng, and F. Bao. Fortifying password authenticationin integrated healthcare delivery systems. In Proc. ASIACCS'06, pages 255-265,2006.

[9] O. Goldreich and Y. Lindell. Session-key generation using humanpasswords only. In Proc. Crypto'01, pages 408-432, 2001.

[10] L. Gong, T. M. A. Lomas, R. M. Needham, and J. H. Saltzer.Protecting poorly-chosen secret from guessing attacks. IEEE J. onSelected Areas in Communications, 11(5):648-656, 1993.

[11] S. Halevi and H. Krawczyk. Public-key cryptography and passwordprotocols. ACM Transactions on Information and SystemSecurity, 2(3):230-268, 1999.

[12] D. Delen, G. Walker, A. Kadam, Predicting breast cancer survivability: a comparison of three data mining methods, Artif. Intell. Med. 34 (2005) 113–127.

[13] Zhou Bodong, Xu Jie, Tian Ye, Yuan Shuai, Xubin Li, Correlation between radiomic features based on contrast-enhanced computed tomography images and Ki-67 proliferation index in lung cancer: a preliminary study, Thorac. Cancer 9 (2018) 1235–1240.