International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

A USER-CENTRIC DATA SECURE CREATION SCHEME IN CLOUD COMPUTING

M.SHUSHEELA[1], L.KIRAN KUMAR REDDY[2]

[1]Pursuing M.Tech (CSE), [2]Working as an Assistant Professor & HOD Department of CSE,
Visvesvaraya College of Engineering & Technology, Affiliated to JNTUH, TELANGANA, (INDIA)

ABSTRACT

The use of the cloud computing technology, the ownership is separated from the administration of the data in cloud and the shared data might bemi grated between different clouds, which would bring new challenges to data secure creation, especially for the data privacy protection. We propose a User-centric data secure creation scheme (UCDSC) for the security requirements of resource owners in cloud. In this scheme, a data owner first divides the users into different domains. The data owner encrypts data and defines different secure managing policies for the data according to domains. To encrypt the data in UCDSC, we present an algorithm based on Access control conditions proxy re-encryption (ACC-PRE), which is proved to be master secret secure and Chosen-cipher text attack (CCA) secure in random oracle model. We give the application protocols and make the comparisons between some existing approaches and UCDSC.

Key words — User-centric, ACC-PRE, Data creation, Master secret secure, CCA. In this paper we use a security analysis of algorithm .In this paper we focus on how a mediator can help a social affair of customer to totally utilize the volume markdown assessing philosophy offered by cloud organization providers through financially savvy online resource booking.

I.INTRODUCTION

Cloud computing promotes the sharing and spreading of information in network. According to its characteristics, the ownership is separated from the administration of the data in cloud, which does not only provide the convenience to the users, but also bring some serious challenges to the data privacy protection at the same time. The cloud protects confidentiality, integrality and availability of data[1] based on some cryptographic primitives. The researches on the data security management in cloud computing focus on three aspects, e.g., secure creation, controllable usage[2] and trusted destruction[3], in which the secure creation supports the other two. In order to protect the data hosted in cloud, data owners will encrypt their data before uploading generally. Attribute based encryption (ABE) has been widely used in data encryption in cloud, which is able to accommodate the requirement of access control. Sun *et al*. proposed a cipher text access control mechanism based on the Cipher text policy-attribute based encryption (CP-ABE) algorithm[4].CP-ABE is

regarded as one of the most suitable technologies for data access control in cloud storage. Yang *et al*. designed an access control framework for multi authority systems based on CP-ABE[5]. The researches above-mentioned could provide theoretical proofs for encryption algorithms of data secure creation.

Currently, the resource is almost encrypted and uploaded by the data owner. With the amount of data increases, the higher computing ability of data owner is required .The Proxy re-encryption (PRE)technology could be used to solve the problem of large calculation, which also provides the theoretical support for implementations of ABE and Identity based encryption (IBE)[6] in cloud computing environment. For the demand of fine-grained information management, a new scheme called type based PRE mechanism was proposed in Ref.[7]. It refines the access control of resource by dividing plaintext into different types and encrypts it by different private keys. Tang *et al*. proposed two type-based PRE schemes of Chosen- issued by owners. For example, when a patient is transferred for further treatment, the medical record will been changed between different clouds for health care, while it will also be migrated through the clouds of health care and cloud of insurance for the management of medical insurance. On the other hand, the CSPs might issue the data migration between public clouds for their storing requirement. For instance, CSP*i* would rent a server of CSP*j* for data redundant backup and protection. Further more, the network sharing will also result in the data migration. example, the academic search engine might accelerate the exchanging process of the education information cached in the clouds. In conclusion, the reasons for data migrations mainly include data owner, CSPs and data usage in the network.

Based on the analysis above-mentioned, the cloud data could be created by the data owner and CPSs. The owners could classify, package, encapsulate and encrypt their data to be the specified format at first. Then they publish it to the cloud server. CSPs could integrate, re-package or combine the data dynamically according to the users' requirements, and the data of combining type is produced, which depends on the data of owners and should get their permissions.

The CSPs is the re-creator and manager of data. Therefore, the creation scheme proposed in this paper is designed for the data owners' creation, and the access control conditions will be introduced to the encryptions of creation. The system model mainly includes the resource owners, CSPs and users, in which the servers of CSPs include content managing server, identity authentication server, and data server. The content managing server deals with the requirements of data creating or users' accessing. The identity authentication server takes charge in authenticating user's identities. The data server is responsible for storing the encrypted data and its policies. The resource owners are responsible for the data creation. The data includes the digital content and the corresponding policies. Owners encapsulate the data, divide the users' domain, and upload the encrypted data to the data server via communication channel with the content server. general user wants to apply the permission of accessing particular resource, he will send requirement to the current domain. The domain then sends the user's requirement with some other information about access when a on trot the content server for further authentication. The content server will deal with the requirement with the identity server according to the secure requirement of domain, *e.g.*, identity, role, temporal state, platform, network *etc*.

Finally, the content server returns the result back to the user according to the policy description. It gives the accessing the data server to the corresponding user. Furthermore, the proposed model will

design the server the plaintext/cipher text according to access control conditions, which is proved to be CCA secure and master secret secure. The application protocols are based on the mature cryptographic technologies which are able to protect the confidence and integrity of data, and prevent hostile replay hacking. Comparisons of the proposed scheme with the current researches will be given.

The rest of this paper is organized as follows. Section II presents the security scenario analysis and system model of the UCDSC scheme. In Section III, the algorithm and corresponding application protocols for the proposed scheme are presented. In Section IV, the security analysis is given. In Section V, we make the comparisons. Finally, Section VI concludes the paper.

II. SCENARIO ANALYSIS AND SYSTEM MODEL:

1. The analysis of the cloud data migration ways and data creation types

The ownership of the data is separated from the administration in cloud. The resources, data and services are provided to users in the form of virtualization. Due to the above situations, the problem of privacy protection becomes more serious. It is important to analyze the ways to the data migration for the cloud data protection. It will reflect the secure problems of and requirements for the data distribution and usage. Fig.1 illustrates a typical application scenario of the data usage through the different clouds. Although there are a plenty of Cloud service providers (CSPs) in clouds who construct and maintain the public clouds, there exist some private clouds in different industries, companies and institutes, such as the clouds for healthcare, education, insurance, and finance.

Advantages:

1. Here utilizing this (ROSA) calculation we include the cost effective framework utilizing here straightforwardly client can choose markdown offers without cloud merchant inclusion.

2. Here we concentrate on how an intermediary can enable a gathering of clients to completely use the volume to rebate cost procedure offered by cloud benefit providers(CSP) through cost-effective online asset planning

Disadvantages:

1.This system cloud service provide different pricing strategies as you use as pay less unit for use less.

2. Here user can lost the money and data and time also.

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

III. SYSTEM ARCTECHTURE

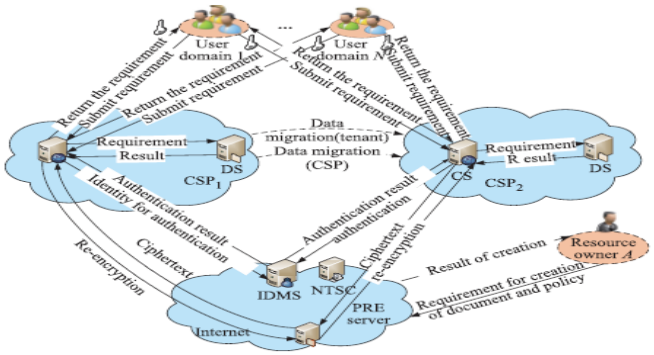

Fig. 1. The system model for UCDSC

IV. THE CONSTRUCTION OF UCDSC:

1. Access control condition

By combining the traditional access control model with the requirements for data secure management, we conclude the access control conditions into 2 types of subject and object. The subject types is consisted of role, identity, time and environment. The object types include attribute, validity and lifecycle. In addition, the conditions might involve security levels, categories, and direction of data stream for consideration of the multi-level security. The ACC-PRE proposed in this section is mainly for the model in Fig. The conditions are introduced for the key construction in encryption and decryption. Therefore, the conditions in this paper are mainly focused on the subjects.

2. Algorithm description of the UCDSC scheme

1) Fundamental definition

Based on the above-mentioned analysis, the algorithm

description of the UCDSC scheme in cloud mainly includes the following 7 functions. In order to describe the construction, let us assume that *i* and *j* denote the creator and the user of data respectively.

1 *_Setup*(*K*) → *param*: Given a security parameter *K* as input, the algorithm outputs the public security parameters*param*.2 *_KeyGen*(*param*) → (*ski, pki*): Given *param*, the algorithm outputs the public and private key pair.3 *_Enc*(*m, pki*) → *Ci*: Given the plaintext *m* and public key *pki* as input, the algorithm outputs the ciphertext*Ci*.4 *_ReKeyGen*(*ski, pkj , condition*) → *rk condition i→j* :Given the private key, public key and condition as input, the algorithm outputs the re-encryption key on condition.5 *_ReEnc*(*Ci, rk conditioni→j*) → *Cj*: Given *Ci* and proxy re-encryption key as input, the algorithm outputs *Cj*. The cipher text can be decrypted by *skj* and *condition*. *_Dec*1(*ski, Ci*) → *m*: Decrypts *Ci* with *i*'s privatekey.7 *_Dec*2(*skj, Cj , condition*) → *m*: The general user*j* decrypts *Cj* by *condition* and *skj* .2) Encryption scheme

Bilinear Groups: $G1$ and $G2$ are two multiplicative cyclic groups of prime order p, and g is a generator of $G1$. $e : G1 \times G1 \rightarrow G2$ is a computable bilinear map with the following properties:

1 _Bilinear: For all $a, b \in Z* p$, we have $e(ga, gb) = e(g, g)ab$.2 _Non-degenerate: $e(g, g) \_= 1$.

V.DBDH (DECISIONAL BILINEAR DIFFIE-HELLMAN) PROBLEM

$c5 = H4(c1\ \ c2\ \ c3\ \ c4)r$

4 _*ReKeyGen*(ski, pkj , *condition*) → *rk conditioni→j* , this algorithm generates the re-encryption key based on Given _$g, ga, gb, gc, e(g, g)abc$_ for some $a, b, c \in$

$Z* p$, $z = abc \bmod p$, a polynomial- time algorithm A has advantage ε in solving the DBDH problem,

if and only if $|Pr[A(g, ga, gb, gc, e(g, g)abc) = 0] - Pr[A(g, ga, gb, gc, e(g, g)z) = 0]| \leq \varepsilon$. To perfect the system above-mentioned, we will propose an ACC-PRE algorithm for UCDSC based on the

DBDH problem as follows. 1 _*Setup*(K) → *param*, this algorithm picks a K-bit prime p. $G1$, $G2$ are multiplicative cyclic groups of prime order p and g is a generator of $G1$. There are four hash functions $H1,H2,H3,H4$ with $H1 : \{0, 1\}* \rightarrow G1$, $H2 : \{0, 1\}* \rightarrow Z* p$, $H3 : G2 \rightarrow \{0, 1\}l$, $H4 : \{0, 1\}* \rightarrow G1$. It outputs public parameters $param = \{p,G1,G2, g,Hi(i = 1, \cdots, 4)\}$.Let us make an assumption that the access control conditions set $condition = \{0, 1\}*$, bilinear map $e : G1 \times G1 \rightarrow G2$.2 _*KeyGen*($param$) → ($ski$, pki), this algorithm picks$xi, xj \in Z* p$, and outputs $ski = xi, pki = gxi$,$skj = xj$,$pkj = gxj$ .3 _*Enc*(m, pki) → Ci: according to this algorithm,user i uses his public key pki to encrypt plaintext m. This algorithm picks $k \in G2$ to compute $r = H2(m\ \ k)$, and outputs $Ci = (c1, c2, c3, c4, c5)$.

$c1 = gr c2 = k \cdot e(pki, H1(pki))r c3 = m \oplus H3(k)$

$c4 = H1(pki)$

condition, pkj and ski, and outputs the re-encryption key $rk\ conditioni \rightarrow j = (pkj, pkrj, H1(pkj\ \ condition) \cdot H1(pki)ski, g-r)$.5 _*ReEnc*($Ci$, *rk conditioni→j*) → Cj,this algorithm outputs a cipher text Ci based on re-encryption key, where $Cj = (c\_1, c\_2, c\_3, c\_4, c\_5)$ if $e(c1, H4(c1\ \ c2\ \ c3\ \ c4)) = e(g, c5)$, otherwise, outputs the error information. The cipher text Cj can be decrypted with skj .

$c\_1 = c1$

$c\_2 = c2 \cdot e(pkrj\ g-r, H1(pki)-ski) \cdot e(pkr$

$j, H1(pkj\ condition) \cdot H1(pki)-ski) = k \cdot e(pkrj, H1(pkj\ \ condition))$

$c\_3 = c3$

$c\_4 = H1(pkj)$

$c\_5 = H4(c\_1, c\_2, c\_3, c\_4)r$

6 _*Dec*1(ski, Ci) → m, his algorithm recovers m by user i's private key as follows: If $e(c1, H4(c1\ \ c2\ \ c3\ \ c4)) = e(g, c5)$, it continues, otherwise, returns error information for integrity.

$k = c2/e(c1, c4)ski$

$m = c3 \oplus H3(k)$

$r = H2(m\ \ k)$

If $c1 = gr$ and $c2 = k \cdot e(g, c4)rski$, then outputs m.

7 _*Dec*2(*skj*, *Cj* , *condition*) → *m*, this algorithm recovers *m* by user *j*'s private key and conditions *condition* as follows: If *e*(*c*_1,*H*4(*c*_1 *c*_2 *c*_3 *c*_4)) = *e*(*g*, *c*_5), it continues, otherwise, returns errors for integrity.

k = *c*_2/*e*(*c*_1,*H*1(*pkj* ||*condition*))*ski*

m = *c*_3⊕*H*3(*k*)

r = *H*2(*m* *k*)

If *c*_1 = *gr* and *c*_2 = *k* · *e*(*pkj*,*H*1(*pkj* *condition*))*r*, then outputs *m*, otherwise, returns error.

Security Analysis:

1.Security analysis of algorithm

DBDH Assumption: We say that the DBDH assumption holds if no probably polynomial-time algorithm (*A*) has advantage *ε* in solving the DBDH problem.2) Security Model of ACC-PRE: Based on the security model of IND-PRE-CCA[13], adversary *A* can query theoracles such as key generation, re-encrypted key generation, re-encryption, decryption and so on. Our proposed scheme will be described as follows Setup: Challenger setups system parameters *param*. Phase 1: Adversary can query one of the any oracles as follows: *KeyGen*, *ReKeyGen*, *ReEnc*, *Dec*1, *Dec*2. During the querying of *ReKeyGen*, *ReEnc*, *Dec*1,*Dec*2, *A*'s private key is generated by *KeyGen*. Challenge: When *A* finishes Phase 1, the challenger picks and outputs *m*0,*m*1 ∈ *M*, access control condition *condition*∗ and a target public key *pk*∗ generated by *KeyGen*. Its corresponding private key is undisclosed. When *A* queries *ReKeyGen* with (*pk*∗ ,*pk*_,*condition*∗),the private key corresponding with *pk*_ should be undisclosed. Challenger picks *b* ∈ {0, 1} randomly and computes *Cb* =*Enc*(*mb*, *pk*∗) as the challenge to *A*.

Phase 2: *A* is allowed to continue querying the sametypes of oracles as in Phase 1. At the end of Phase 2, wehave the following constraints.1 _If *A* queries *ReKeyGen* with (*pk*∗ ,*pk*_,*condition*∗),the corresponding private key is undisclosed.2 _If *A* queries *ReEnc* with (*Cb*,*pk*∗ ,*pk*_,*condition*∗),the corresponding private key is undisclosed.3 _*A* cannot query *Dec*1 with (*C_b*,*pk*∗) directly.4 _If *A* queries *ReKeyGen* with (*pk*∗ ,*pk*_,*condition*∗),

A cannot query *Dec*2 with *C_b*, where *C_b* is valid.Guess: *A* outputs a guess, if *b*_ = *b*, *A* will success.

Let us define the advantage of *A* to success as *ε*, where*ε* = |*Pr*[*b*_ = *b*]− 12|. If *ε* is negligible, *A* will fail. It meansthat the ACC-PRE is CCA security.

Theorem:

If DBDH assumption holds in groups (*G*1,*G*2), then the ACC-PRE is CCA secure based on random

oracle model.

Proof sketch:

This theorem means that if *A* challenges with the advantage

ε, then $\varepsilon = |Pr[b\_ = b] - 12|$ is negligible. Let us define challenging games as $Gi(i = 1, \cdots, 6)$, and challenger as $B.Ti$ denotes the event which will happen when $b\_ = b$ in Gi._1 $G0$: Challenger B faithfully answers the oracle queries from A. At the same time, B initializes $Hlisti$ (i =1, · · · , 4) by choosing $\pi 1, \pi 4 \in G1, \pi 2 \in Z* p$, $\pi 3 \in \{0, 1\}l$and setting (pki,$\pi 1$),(m,k,$\pi 2$),(k,$\pi 3$), ($c1$,$c2$,$c3$,$c4$,$\pi 4$) in

$Hlisti$ ($i = 1, \cdots, 4$). Let $\delta 0 = Pr[b\_ = b]$, then $|\delta 0 - 1$

$2| = \varepsilon$._2 $G1$: Challenger B does the same as that in $G0$, except the following:B randomly picks $\tau \in \{1, 2, \cdots, p + 1\}$ to query $H1$ in τ times. When B receives A's challenge to query $H1$,B aborts the game. Therefore, the probability of B to succeed is 1

p+1 at least. $\delta 1 = Pr[b\_ = b]$ in $G1$, and then

$Pr[T1] = \delta 1p+1$._3 $G2$: Challenger B does the same as that in $G1$, except the situation of Hi conflicting. The hash function sare the standard random oracles, so $|Pr[T1] - Pr[T2]|$ is negligible.

4 $G3$: Challenger B does the same as that in $G2$, except the query of $Dec2$. In the oracle of $Dec2$ querying,

if the input is (C,$pk*$,$condition*$) and A has not queried $H1$ with ($pk*$ $condition*$), then B aborts the

game, otherwise B returns the cipher text to A. Since the hash functions are the standard randomoracles and all the cryptography algorithms are certain, $|Pr[T2] - Pr[T3]|$ is also negligible.

5 $G4$: Challenger B does the same as that in $G3$,except the query of $Dec1$. If A has not queried $H2$ with

mb $k*$, there is no differences between $G4$ and $G3$. There

fore,$|Pr[T3] - Pr[T4]|$ is negligible.

6 $G5$: Challenger B does the same as that in $G4$, except the querying of $ReKeyGen$ and $ReEnc$. During

the query, B searches the re-encryption key list with (pki,pkj ,$condition$) proposed by A. If there is a result of

search, B will return $rkcondition$ $i \rightarrow j$ to A, otherwise, B will continue as follows. If user i's private key is corrupted,which means $ski - xi$, then B computes $rkconditioni \rightarrow j$ =(pkj, $pkrj$,$H1$(pkj ||$condition$) · $H1$(pki)ski, $g-r$)

If user i's private key is uncorrupted, then B willpick $a \in G1$, set $ski = axi$, and compute $rkcondition$

$i \rightarrow j$ =(pkj, $pkrj$,$H1$(pkj ||$condition$) · $H1$(pki)ski, $g-r$).If j's private key is corrupted, then B aborts. When $ReEnc$ is being queried, B computes the re encryption cipher text under condition of $ReEnc$ with (pki, pkj, Ci) proposed by A. If it does not hold, B aborts. Otherwise, B searches the private keys from private key

list and re-encryption key list, and returns ciphertext to *A*. If *pkj* is not generated by *KeyGen*, *B* aborts.

$|Pr[T4] - Pr[T5]|$ is negligible as that in Ref.[7].

7 $G6$: Challenger B does the same as that in $G5$, except the following situations. When B receives the A's challenging $(m0,m1,condition)$,B will decrypt the cipher text at first time, and then pick $b \in \{0, 1\}$ to compute $k \in G2$, $r = H2(mb||k)$,$c1 = gr$, $c2 = k \cdot e(pki,H1(pki))r$, $c3 = m\_H3(k)$,$c4 = H1(pki)$, $c5 = H4(c1||c2||c3||c4)r$. Therefore, the difference between $G6$ and $G5$ is whether query $H3$ or not. The difficulty of querying $H3$ is based on the DBDH problem, so $|Pr[T5] - Pr[T6]|$ is negligible. Hash functions are the random oracles, so $Pr[T6] = 12(p + 1)|Pr[T1]-Pr[T6]| = |Pr[T1]- 1$

$2(p + 1)|$ is negligible base don the analysis from 1 _ to 7 _ , the $Pr[T1] = \delta 0$

$p + 1$and$| 2\delta 0 - 12(p + 1)| = | \delta 0 - 1$

$2(p + 1)| = | \varepsilon(p + 1)|$ is negligible. There fore,ε is negligible. The proof is finished.

VI.CONCLUSIONS

In this paper, we proposed a UCDSC scheme in cloud, according to which the users could be divided into different domains and the access control policies are able to be assigned for the domains. Furthermore, we presented an ACC-PRE for the algorithm for the UCDSC scheme, which introduces the access control conditions. to construct the re-encryption keys. The ACC-PRE can reduce the computational overhead of the user's encryption and difficultly of key management, and satisfy the users' requirements for dynamical adjustment of permission descriptions as well. Then we gave the corresponding application protocols, which are able to protect the data during storing and communicating. Finally, the result of the security analysis and comparison with other schemes indicates that the UCDSC scheme is secure, practical and flexible in cloud.

REFERENCS:

[1] Y. Fu, S. Luo and J. Shu, "Survey of secure cloud storage systemand key technologies", Journal of Computer Research and Development, Vol.50, No.1, pp.136–145, 2013. (in Chinese)

[2] M. Su, F. Li, Z. Tang, et al., "An action-based fine-grained access control mechanism for structured documents and its application", The Scientific World Journal, Vol.2014, pp.1–13, 2014.

[3] J. Xiong, F. Li, J. Ma, et al., "A full lifecycle privacy protection scheme for sensitive data in cloud computing", Peer-to-Peer Networking and Applications, pp.1–13, 2014.

[4] G. Sun, N. Dong and Y. Li, "CP-ABE based data access control for cloud storage", Journal on Communications, Vol.32, No.7, pp.146–152, 2011. (in Chinese)

[5] K. Yang and X. Jia, "Attributed-based access control for multi authority systems in cloud storage", Proc. of the International Conference on Distributed Computing Systems, Macau, China,pp.536–545, 2012.

[6] J. Xiong, Z. Yao, J. Ma, et al., "A secure self-destruction with IBE for the internet content privacy", Chinese Journal of Computer, Vol.37, No.1, pp.139–150, 2014. (in Chinese)

[7] Q. Tang, "Type-based proxy re-encryption and its construction", Proc. of the International Conference on Cryptology in India: Progress in Cryptology, Kharagpur, India, pp.130–144, 2008

[8] J. Zhao, D. Feng, L. Yang, et al., "CCA-secure type-based proxy re-encryption without pairings", Acta Electronic a Sinica, Vol.39, No.11, pp.2513–2519, 2011. (in Chinese) [9] X. Wang and W. Zhong, "A new identity based proxy re encryption scheme", Proc. of the International Conference on Biomedical Engineering and Computer Science, Wuhan, China, pp.1–4, 2010.

[10] X. Liang, Z. Cao, H. Lin, et al., "Attribute based proxy re encryption with delegating capabilities", Proc. of the International Symposium on Information, Computer, and Communications Security, Sydney, Australia, pp.276–286, 2009.

[11] J. R. Douceur, A. Adya, W. J. Bolosky, D. Simon, and M. Theimer, "Reclaiming space from duplicate files in a serverless distributed file system," Proc. International Conference on Distributed Computing Systems (ICDCS), pp. 617–624, 2002.

[12] S. Halevi, D, Harnik, B. Pinkas, and A. ShulmanPeleg, "Proofs of ownership in remote storage systems," Proc. ACM Conference on Computer and Communications Security, pp. 491–500, 2011.

AUTHOR DETAILS:

	**M SHUSHEELA** Pursuing M.Tech (CSE), (15BT1D5823) from Visvesvaraya College of Engineering & Technology, M.P. Patelguda, Ibrahimpatnam, Hyderabad,Telangana , Affiliated to JNTUH, India.
	**Mr. L.KIRAN KUMAR REDDY** Working as an Asst. Professor and HOD of CSE Department in Visvesvaraya College of Engineering & Technology, M.P. Patelguda, Ibrahimpatnam, Hyderabad, Telangana , Affiliated to JNTUH, India.