International Journal of Trend in Scientific Research and Development (IJTSRD)

International Open Access Journal

ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 5

Security Enhancement Using NTRU Algorithm Based Cryptosystem for Communication of Classified Information Via Cloud

Aishwarya Rani M R[1], Gururaj Gowda Patil M[1], Mr. Shivanand R D[2]

[1]Student, [2]Associate Professor

[1,2,3]Department of Computer Science and Engineering

Bapuji Institute of Engineering and Technology, VTU, Davanagere, India

ABSTRACT

Distributed storage depends on exceptionally artificial foundation and encourages available boundary point, flexibility and versatility it can oversee profoundly dimensions and tedious information. Henceforth, subcontracting encoded text to a cloud is ended up being a standout amongst the best methodologies for big data stockpiling and admittance. In spite of the fact that gives bounteous security highlights, it is important to verify the client to the most elevated degree with no need of trading off effortlessly utilization and furthermore protected refreshing the encoded text in the cloud in light of another entrance approach as assigned by the information proprietor. These two necessities posture to be a noteworthy test to make the capacity more compelling. There is no real advancement in the territory of admittance approach in the vibrant condition by the conventional frameworks. Now a days, ingression arrangement refresh is critical for improving protection and managing great recurrence of client development. The undertaking goes for executing a protected and obvious admittance organize plot in light of the NTRU encryption algorithm. The deficiency of the current NTRU frameworks will be assessed for corresponding decoding ability and as needs be another NTRU unscrambling calculation will be tried to defeat the unscrambling disappointments of the first NTRU. The plan is exceedingly delicate to the approach refresh it will enables the cloud server to successfully refresh the encoded text when another entrance strategy is indicated by the information proprietor. It likewise empowers (i) the information proprietor and qualified clients to successfully assess the authenticity of a client by check of qualifications and (ii) a client to approve the data gave by different clients to revise original recuperation. Pre-examination investigation of the plan demonstrates that it will keep qualified clients from swindling and give protection from attacks, for example, the plot assault.

Keywords: *NTRU algorithm, Big data, Cloud, Encryption.*

I. INTRODUCTION

Big Data is a phrase it alludes towards information groups or blends of information collection its dimension, intricacy, and corresponding speed of development lead them hard to caught, overseen, handled or investigated down through traditional knowledge and devices, for example, relational databases and work area insights or representation bundles, inside the occasion important mainly to create them helpful. Difficulties intended for the Big Data incorporate examination, catch, information span, seek, distributing, stockpiling, exchange, perception, questioning, refreshing and data security.

Because of its many sided quality and extensive volume, overseeing Big Data utilizing close by database administration apparatuses is troublesome. A compelling arrangement is mainly to provide subcontract the information toward the cloud server so as to the abilities of putting away Big Data and preparing clients' entrance asks for in a proficient way. For instance, an e-wellbeing applications, the genome data ought to be safely put away in an e-wellbeing cloud because a solitary progression individual genome be approximately 140 gigabytes in an estimate [1]. In any case, while an information proprietor subcontract associated information in the direction of a cloud, delicate data might be unveiled in light of the fact that the cloud server is not faithful and conviction; along these lines, commonly the encrypted text of the information is put away into the cloud [1]. Be that as it may, how to refresh the encrypted text or cipher text put away into a cloud when another entrance approach is assigned through the statistics proprietor and to confirm the authenticity of a client who expects toward get to the information be at a standstill of extraordinary distress.

A large amount of obtainable methodologies for protecting the outsourced Big Data in mists depend resting on moreover Attribute based encryption (ABE) or mystery sharing. ABE foundational methodologies give the adaptability to an information proprietor to predefinition the arrangement of clients the one is qualified in favor of getting to the information. Mystery distributing instruments enable a secrete on the way to be communal and recreated via firm figure of helpful clients, yet they ordinarily utilize lopsided open key cryptography, for example, RSA for clients' authenticity check, it causes elevated calculation visual projection.

The most testing matter is the means by which to check the authenticity of the clients getting to the subcontracted information in clouds. At present available plans proposed in [1] don't bolster client qualification check. Then again, evident secret distribution construct plans depend with respect to RSA [1] meant for get to authenticity check. Because of various clients require to commonly confirm every other utilizing different RSA activities, equivalent techniques have an elevated statistical visual projection. Moreover, the great asymmetric algorithm for cryptography arrangements, for example, RSA might be out of order through quantum registering sooner rather than later.

The NTRU is an acronym for **Nth degree Truncated polynomial Ring Unit** [9]. The principle trademark be with the intention of amid the encoding and decoding the polynomial duplication is the majority tedious task. This is substantially rapid compare to other deviated cryptosystems, for example, RSA [9]. The NTRU methodology for cryptosystem is a kind of cross section foundational cryptography, and corresponding security depends on top of the briefest vector problem (SVP) in a grid [1]. The significant points of interest of NTRU be portion figuring assault opposition and illumination of a quick calculation ability.

An enhanced NTRU methodology for cryptosystem (Improved RNS Algorithm) has been projected to defeat the unscrambling disappointments of the first NTRU. At that point a safe and obvious plan in view of the enhanced NTRU and mystery distributing meant for Big Data stockpiling is planned. The cloud server be able to straight forwardly refresh the put away encrypted text or cipher text exclusive of decoding in view of the new access approach determined by the information proprietor, who can approve the restore at the cloud. The anticipated plan be able to confirm the mutual mystery data to keep clients from deceiving and be able to counter different assaults, for example, the intrigue assault. It is additionally esteemed toward be there secure regarding dimension registering assaults because of NTRU.

II. LITERATURE SURVEY

Researchers and specialists posses the chance to modify the range of center by examining the gigantic statistics grouped by the present civilization. To dissect this kind of liberal level informational records, appropriated preparing has been planned as a fiscally keen and reasonable figuring point of view. Regardless, in the view of fact that information passes on confidential data, it ought to be astound starting the cloud and outer aggressors for good, protection, or true blue reasons. Additionally, it has been observed that some expansive level of information examination strategies depend upon second a large amount of key calculation issues, i.e., facilitate variable based math and streamlining and the basic problem and test for flowed handling is the protection of the cloud condition, a broad assortment of rationalities and dimensions have as of late it's been projected by different specialists. Cloud associations suppliers are before long pursuing down the best protection and defense instruments it would create the cloud air protected and ensured intended for their relative clients and it will keep up the complete assurance above the cloud ace affiliation.

Problem Statement

The current Attributed-based encryption (ABE) or mystery distributing frameworks it give verification and adaptability to a information proprietor to predefine the arrangement of clients who are qualified for getting the information however encounter a misfortune amid its vibrant working that includes standard refreshing of the entrance approach accordingly producing enormous data. The work of asymmetric public key cryptography, for example, RSA intended for client validation causes huge calculation transparency for this situation. The remedy to this problem lies in implementing an algorithm based on a technique that involves regular ingression policy update, which is highly sensitive to intruder attack and also capable of complex data computation in a dynamic environment. The current Attributed-based encryption (ABE) or mystery distributing frameworks it give verification and adaptability to a information proprietor to predefine the arrangement of clients who are qualified for getting the information however encounter a misfortune amid its vibrant working that includes standard refreshing of the entrance approach accordingly producing enormous data. The work of asymmetric public key cryptography, for example, RSA intended for client validation causes huge calculation transparency for this situation. The remedy to this problem lies in implementing an algorithm based on a technique that involves regular ingression policy update, which is highly sensitive to intruder attack and also capable of complex data computation in a dynamic environment.

Objectives

The fundamental target of the framework mainly to suggest a protected and irrefutable admittance manage plot intended for the technology Big Data stockpiling located at cloud server and handling the difficulties of the accompanying security administrations:

- ➢ To contemplate and break down the present critical admission strategies designed for their deficiencies and pragmatic issues.
- ➢ To provide high security, entirely bearing in mind the security of the data storage such that sensitive information is not vulnerable.
- ➢ To demonstrate that proposed scheme can resist various attacks such as the collusion attack via a rigorous analysis.

III. METHODOLOGY

Key, individuals who coordinate through dispatcher be able to refresh sender's information on the cloud server. When sender will distribute a group S of its information with collector, it can figure the total key KS for recipient through the stage of fetching function is similar to Extract (MSK, S). Because KS is only a steady dimension key, it is anything but difficult near be sent to beneficiary by means of a protected email.

IV. ARCHITECTURE

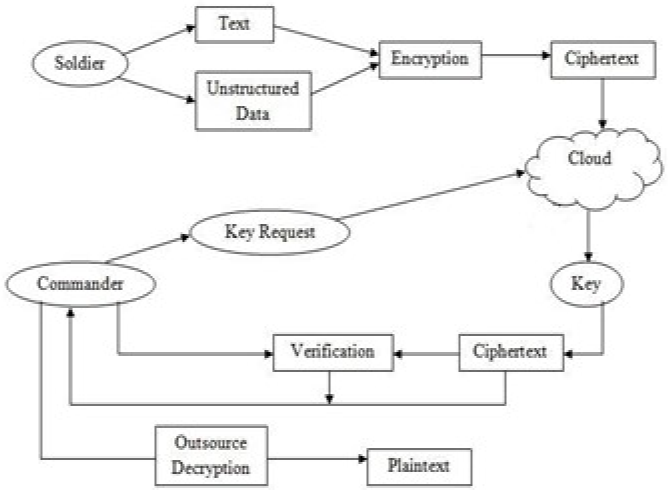


Figure 1: Secure and Verifiable access control methodology

The figure 1 illustrates the secure and verifiable access control methodology. Planned arrangement scheme consists of three polynomial-time algorithms as follows:

- Key Generation Step
- Encryption Step
- Decryption Step

- ➢ The information proprietor sets up the general population framework arguments by means of association and creates an open or master security key combine through Key production. Communication knows how to encode by means of Encrypt by any individual who likewise chooses what figure content class is related through the normal text communication to be scrambled.
- ➢ The information proprietor be able to utilize the master security key to produce a total decoding key for an arrangement of encrypted cipher text classes through Extract. The created or produced security keys be able to share with entrust safely (by means of protected messages or safe and sound gadgets).
- ➢ In conclusion, some client by means of a total key it will be decrypted by any cipher text gave by the cipher text medium is enclosed in the total key by means of Decrypt.
- ➢ Assume dispatcher needs to distribute his information m1, m2, ….mi to the cloud server. To begin with Setup is performed to get arguments

and carry out Key Generation stage mainly to receive people in public or master security key match (PK means of primary key; MSK means of master security key).

- The scrambled information‟s are transferred intended to the server. By means of param and PK it says that primary.

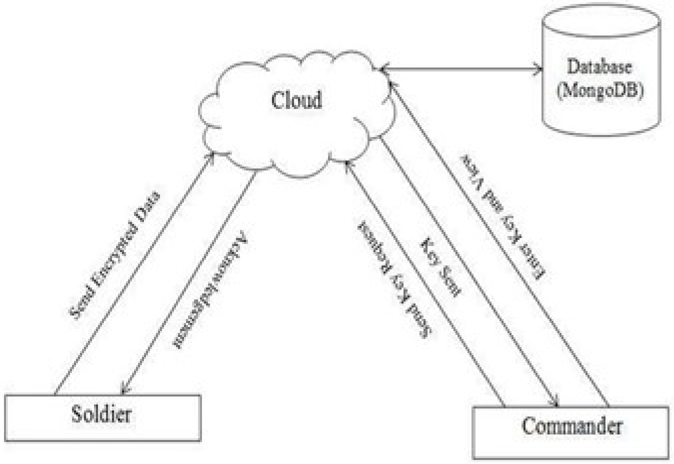


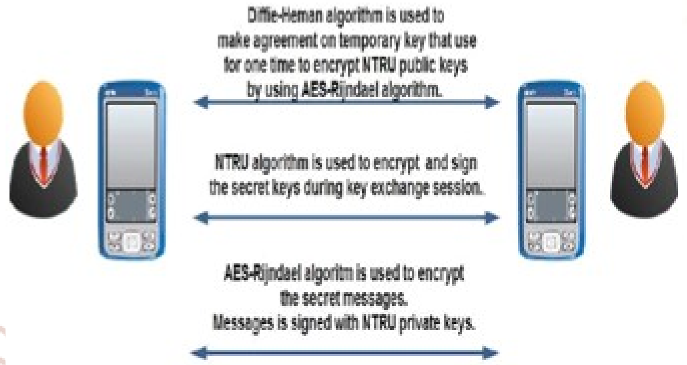
Figure 2: System Architecture

The secure and verifiable access control scheme cryptosystem uses the above system architecture. Application makes use of MongoDB to store and process the data. The frontend of the application is designed using servlet. The proposed system uses NTRU (Nth degree Truncated polynomial Ring Unit) algorithm to encrypt the data and decrypt it using key generated by the NTRU algorithm. Thus the application allows only intended users to get verified access to important data.

Step1: Soldier will upload the data into cloud. Afteruploading data successfully commander will get the intimation mail.
Step2: Commander requests the key from cloud. Key is generated using NTRU algorithm. Once he get the key from cloud he can view the original data.
Step3: Commander will reply to soldier.
Step4: Soldier will view the reply sent by commander.

V. ALGORITHM

NTRU is an acronym it illustrates Nth degree shortened function ring. The important features are that for the duration of the encoding and decoding the function reproduction is the majority tedious complex process. It is a great quicker than additional asymmetric encryption algorithm, for example RSA asymmetric algorithm and elliptic curve encryption algorithm. The NTRU was developed during 1996 by scientists Jeffrey Hoff stein, Joseph H. Silverman, and Jill Pipher. Afterward finally during 1996 scientists besides with Daniel Lieman set up the NTRU encryption algorithm. The scientists were measured on increasing up the procedure.


Diffie-Heman algorithm is used to make agreement on temporary key that use for one time to encrypt NTRU public keys by using AES-Rijndael algorithm.
NTRU algorithm is used to encrypt and sign the secret keys during key exchange session.
AES-Rijndael algoritm is used to encrypt the secret messages.
Messages is signed with NTRU private keys.

NTRU Keys and Parameters

- N - The polynomials in the ring R have degree N-1.
- q - The large modulus to which each coefficient is reduced.
- p - The small modulus to which each coefficient is reduced.
- f - A polynomial that is the private key.
- g - A polynomial that is used to generate the public key h from f (Secret but discarded after initial use)
- h - The public key, also a polynomial
- r - The random “blinding” polynomial (Secret but discarded after initial use)
- d- Coefficient

Key Generation Step

- **Step 1:** User B randomly chooses 2 small polynomialsf and g in the R
- **Step 2:** The inverse of f modulo q and the inverse of f modulo p will be computed
  $f * f_q^{-1} = 1(\text{modulo } q)$ $f * f_p^{-1} = 1(\text{modulo } p)$
- **Step 3:** Product of polynomials will be computed:
  $h = p * ((Fq)*g) \bmod q.$

Encryption Step

- **Step 1:** User A has a message to transmit.
- **Step 2:** User A puts the message in the form ofpolynomial **m** whose coefficients is chosen modulo p between -p/2 and p/2.
- **Step 3:** Randomly chooses another small polynomial **r**.
- **Step 4:** Computes the encrypted message:
  $e = r * h + m \text{ (modulo q)}$

Decryption Step

- **Step 1:** Client B obtains a memo **e** commencing fromA and wants to decode it.
- **Step 2:** By using confidential function polynomial **f**.Client B calculates a function.
- **Step 3:** Client B requires to select constants of **a** thatresides in an intermediate of span **q**.
- **Step 4:** Client B calculates the function b = a (mod p).Client B decreases each and every constants of a mod p.
- **Step 5:** B utilizes the additional confidential functionf$_p$ to calculate c **= f$_p$* b (mod p)**, it is the unique memo of A.

VI. IMPLEMENTATION DETAILS

Software Requirements

Operating System	: Windows 7 and Above
Web Technology	: Servlets, JSP
IDE	: Eclipse Mars
Application server	: Apache Tomcat 8.0
Hadoop Database	: MongoDB
Database Connectivity	: Robomongo-0.8.5-i386

Hardware Requirements

Processor	: Intel I3 and Above
RAM	: 4 GB
Hard Disk	: 500 GB

A. Procedure to upload data

The below described procedure allows soldier to upload data related to current situation. All data will be successfully stored into „report" collection. After the data is successfully uploaded corresponding soldier will be acknowledged.

Input: Data consist of soldier name, communicating mailid, confidential secret id, place, date, document and state.

Process: Uploading soldier information. Information will besaved in report collection.

```
        Create collection db object;
        Construct a mongo client object;
        Fetch the database named "secure data";
        From database get collection report;
        construct basic database object;
        Append soldier information to database such
as name, mail id, confidential id, date, state details;
```

Output: Information uploaded effectively message displayed on the screen.

B. Procedure for data Encryption

The below procedure describes how the uploaded data is encrypted using public key. The encrypted data is stored in „plan" collection.

Input: Information on the way to be encoded. i.e., databaseentities.

Process: Encoding the information via utilizing NTRUinformation encoding step.

Construct a multipart request object y providing parameters name, directory name; Fetch parameter names;

```
        for (var param in parameters)
        {fetch next parameter name;
        if (parameter name == "detail")
        {e = Get multi parameter name;
        Fetch the confidential key;
        Get bytes and fetch AES key;
        Construct encoded text nothing but
        cipher text;
        Initialize cipher text;
        Get bytes associated with the
        cipher text;
        Generates the encrypted text;}
```

Output: Information will be encoded effectively and savesin database.

C. Procedure for Key Generation

The below pseudocode describes the key generation procedure and the generated key is sent to commander mail-id through SMTP protocol. The generated key will be stored in key collection.

Input: Press waiting link button;

Process: Produce the Key

- Generate an integer y random number;
- Convert generated random into to string;
- Set attribute value to mail id;
- create boolean variable session debug and
- assign value to true ;
- Fetch system properties;
- Put host properties values;
- Assign transport protocol value to SMTP; Assign authentication value to true; Assign mail smtp value to true;
- Assign port value as 465; Assign fallback value to "false"; Assign class value to

SSL_FACTORY; Construct a mails session object with props; Assign set Debug to session Debug; Create a new mime object;

- Assign internet address to new mime object;
- Construct internet address array;
- Fetch message recipients;
- Set subject value to msg object; Set content value to msg object; Construct transport object and set value to smtp;
- Connect transport object by using corresponding user name and password;

Output: Key production will be effectively done and savedin database.

D. Procedure for data Decryption

The below procedure describes the data decryption module. Commander decrypts the data by using generated key to view original data.

Input: Cipher text will be given as an input;

Process: Decoding the information through utilizing NTRUinformation decoding step

- Fetch a secrete id value from the request parameter
- Fetch a key value from the request parameter;
- Construct a collection object from the database collection;
- Construct a mongo client object and initialize it with a values;
- Get a mongo client database with a name secure data;
- Fetch user name from the database collection;
- Construct a basic database object with parameters secrete id; Construct a query object;
- Assign secrete id value to query;
- Assign id value to query;
- Search collection to find the query;

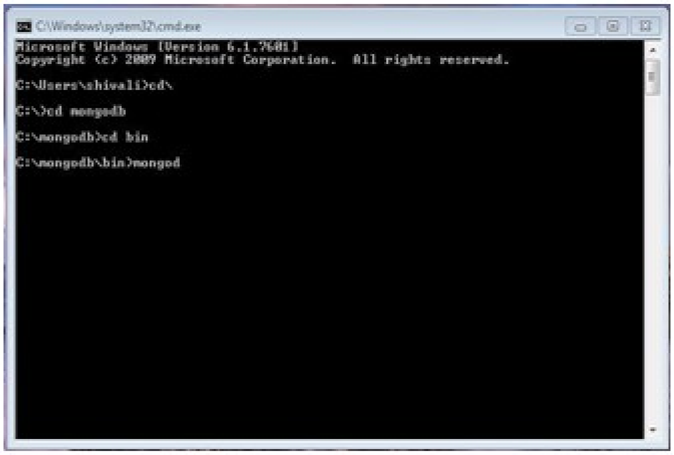
While (until cursor has next)
{display the response from viewport jsp page;}

Display the information saying (entered key is wrong);

Output: Information decoded effectively.

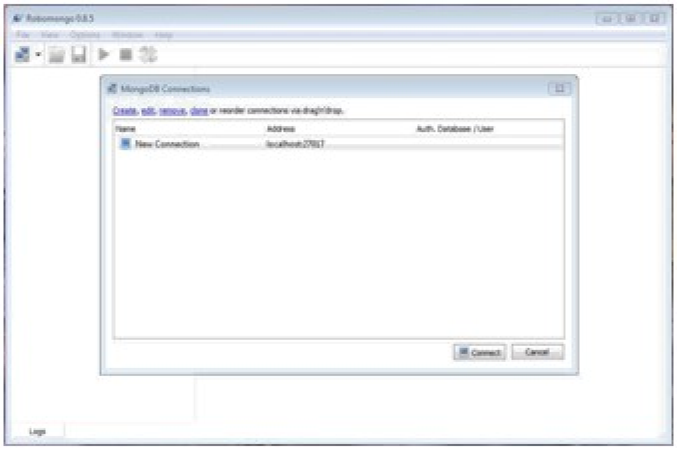
VII. RESULTS

The product is demonstrated module-wise with respect to the users such as soldier and commander. The screen shots given below depict the project results.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\shivali>cd\

C:\>cd mongodb

C:\mongodb>cd bin

C:\mongodb\bin>mongod
```

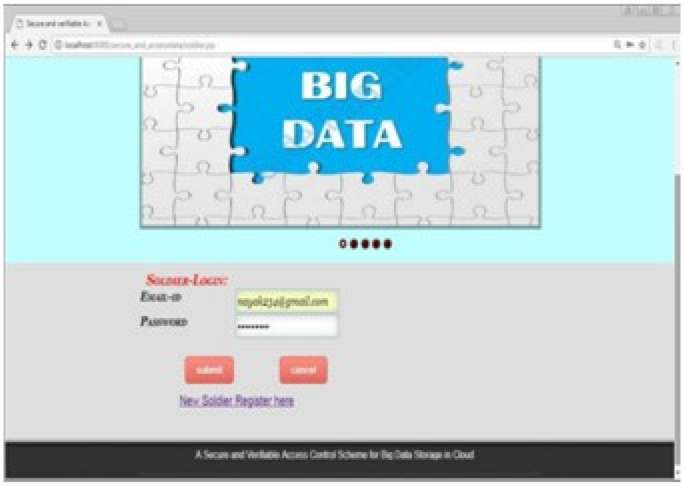
Figure3: Launching MongoDB



Create, edit, remove, clone or reorder connections via drag'n'drop.

Name	Address	Auth. Database / User
New Connection	localhost:27017	

Figure4: MongoDB connection to Tomcat server


BIG
DATA
submit
cancel
New Soldier Register here
A Secure and Verifiable Access Control Scheme for Big Data Storage in Cloud

Soldier-Login:
Email-id nayoliz34@gmail.com
Password ••••••••

Figure5: Soldier Login page

The Soldier has to register if he is a new user. The figure 5 shows the login UI for soldier. The soldier has to enter the valid registered credentials like Email-id and password to upload the text and unstructured data to cloud. On click of submit button soldier will be navigated to user menus page.

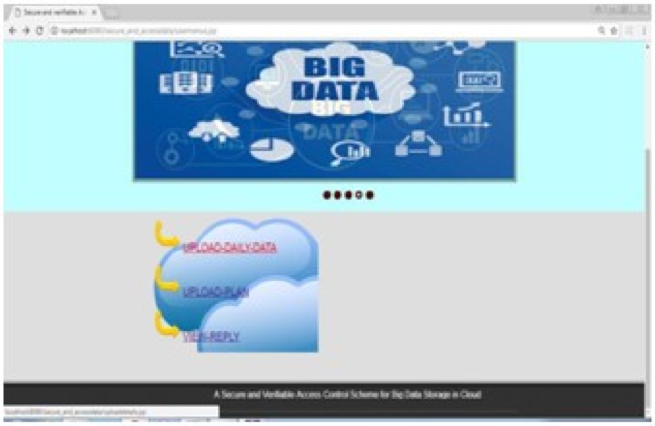
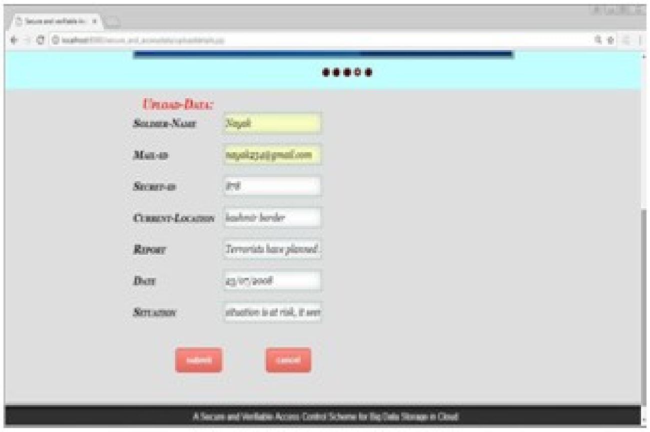

BIG
DATA
UPLOAD-DAILY-DATA
UPLOAD-PLAN
VIEW-REPLY
A Secure and Verifiable Access Control Scheme for Big Data Storage in Cloud

Figure 6: Actions performed by Soldier

The figure 6 shows the list of actions performed by soldier such as upload-daily-data, upload plan and view reply. On click of upload-daily-data link the soldier will be navigated to upload details page and is able to upload data.

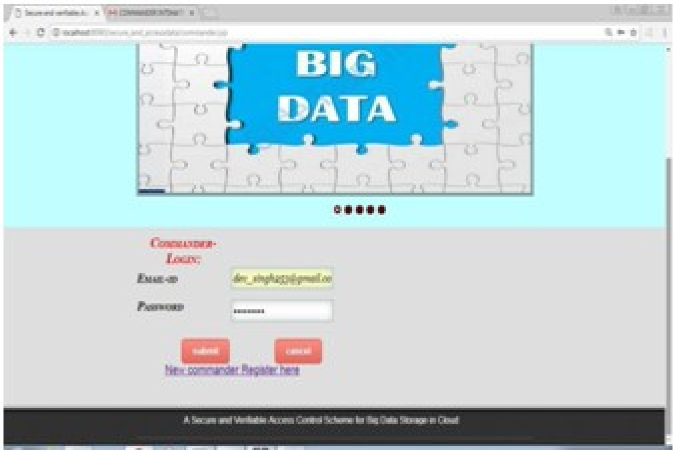

Upload-Data:

Soldier-Name	Nayak
Mail-id	nayak234@gmail.com
Secret-id	878
Current-Location	kashmir border
Report	Terrorists have planned
Date	23/07/2008
Situation	situation is at risk, it see

submit
cancel
A Secure and Verifiable Access Control Scheme for Big Data Storage in Cloud

figure7: Soldier uploads data by entering required, inputs

The figure 7 shows the screen shot of uploading data by soldier. Soldier has to enter secret-id, current location, situation of current location and he has to report. On click of submit button data will be successfully uploaded.



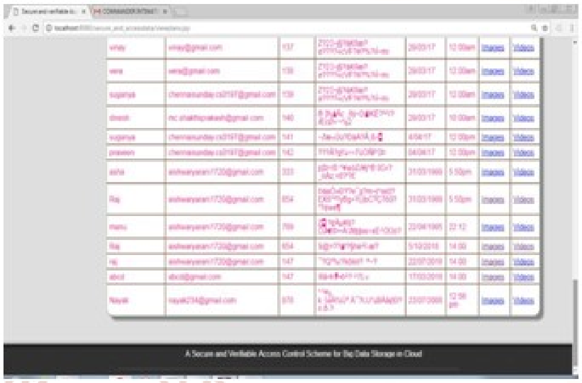
Commander-Login:

Email-id	dev_singh4253@gmail.co
Password	••••••••

submit
cancel
New commander Register here
A Secure and Verifiable Access Control Scheme for Big Data Storage in Cloud

Figure 8: Commander Login page

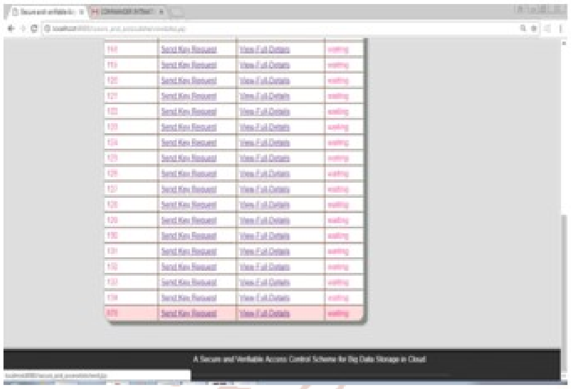
The commander has to register if he is new user. The figure 8 shows the login UI for commander. The commander has to enter the valid registered credentials like email-id and password to view the text and unstructured data. On click of submit button commander will be navigated to commander menus page.



vinay	vinay@gmail.com	137	[illegible]	28/03/17	12:00am	images	Videos
vera	vera@gmail.com	138	[illegible]	28/03/17	12:00am	images	Videos
suganya	chennaisunday.cs2197@gmail.com	139	[illegible]	28/03/17	12:00am	images	Videos
dinesh	mc.shakthiprakash@gmail.com	140	[illegible]	28/03/17	10:00am	images	Videos
suganya	chennaisunday.cs2197@gmail.com	141	[illegible]	4/04/17	12:00pm	images	Videos
praveen	chennaisunday.cs2197@gmail.com	142	[illegible]	04/04/17	12:00pm	images	Videos
asha	aishwaryaram1720@gmail.com	333	[illegible]	31/03/1999	5:50pm	images	Videos
Raj	aishwaryaram1720@gmail.com	654	[illegible]	31/03/1999	5:50pm	images	Videos
manu	aishwaryaram1720@gmail.com	789	[illegible]	22/04/1995	22:12	images	Videos
Raj	aishwaryaram1720@gmail.com	654	[illegible]	5/10/2018	14:00	images	Videos
raj	aishwaryaram1720@gmail.com	147	[illegible]	22/07/2018	14:00	images	Videos
abcd	abcd@gmail.com	147	[illegible]	17/03/2018	14:00	images	Videos
Nayak	nayak234@gmail.com	878	[illegible]	23/07/2008	12:56 pm	images	Videos

A Secure and Verifiable Access Control Scheme for Big Data Storage in Cloud

Figure 9: Screenshot of Encrypted data table



117	Send Key Request	View Full Details	waiting
119	Send Key Request	View Full Details	waiting
120	Send Key Request	View Full Details	waiting
121	Send Key Request	View Full Details	waiting
122	Send Key Request	View Full Details	waiting
123	Send Key Request	View Full Details	waiting
124	Send Key Request	View Full Details	waiting
125	Send Key Request	View Full Details	waiting
126	Send Key Request	View Full Details	waiting
127	Send Key Request	View Full Details	waiting
128	Send Key Request	View Full Details	waiting
129	Send Key Request	View Full Details	waiting
130	Send Key Request	View Full Details	waiting
131	Send Key Request	View Full Details	waiting
132	Send Key Request	View Full Details	waiting
133	Send Key Request	View Full Details	waiting
134	Send Key Request	View Full Details	waiting
878	Send Key Request	View Full Details	waiting

A Secure and Verifiable Access Control Scheme for Big Data Storage in Cloud

Figure 10: Screenshot of view-daily-data table

The figure 10 shows the screenshot of view-daily-data screen. On click of send key request link commander can send key request to cloud to view the data uploaded by corresponding soldier.

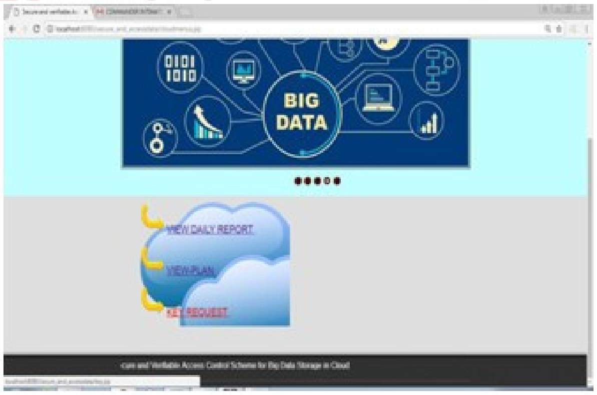
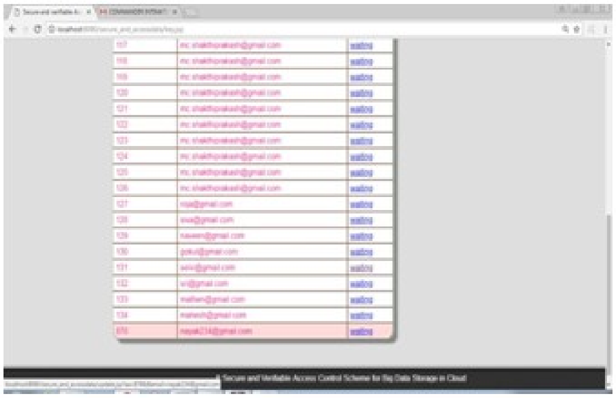

0101
1010
BIG
DATA
VIEW DAILY REPORT
VIEW-PLAN
KEY REQUEST
-cure and Verifiable Access Control Scheme for Big Data Storage in Cloud

Figure 11: Screenshot of Cloud Menus

The user has to login for colud. The figure 11 shows the screenshot of cloud menus such as view-daily-report, view plan and send key to commander. On click of Key request link the key will be generated.



117	mc.shakthiprakash@gmail.com	waiting
118	mc.shakthiprakash@gmail.com	waiting
119	mc.shakthiprakash@gmail.com	waiting
120	mc.shakthiprakash@gmail.com	waiting
121	mc.shakthiprakash@gmail.com	waiting
122	mc.shakthiprakash@gmail.com	waiting
123	mc.shakthiprakash@gmail.com	waiting
124	mc.shakthiprakash@gmail.com	waiting
125	mc.shakthiprakash@gmail.com	waiting
126	mc.shakthiprakash@gmail.com	waiting
127	riya@gmail.com	waiting
128	siva@gmail.com	waiting
129	naveen@gmail.com	waiting
130	gokul@gmail.com	waiting
131	selvi@gmail.com	waiting
132	vi@gmail.com	waiting
133	mathan@gmail.com	waiting
134	mahesh@gmail.com	waiting
878	nayak234@gmail.com	waiting

A Secure and Verifiable Access Control Scheme for Big Data Storage in Cloud

Figure 12: Screenshot of view-daily-data table in Cloud

The figure 12 shows the screenshot of view-daily-data screen. On click of waiting link the generated key will be sent to corresponding commander"s email-id.

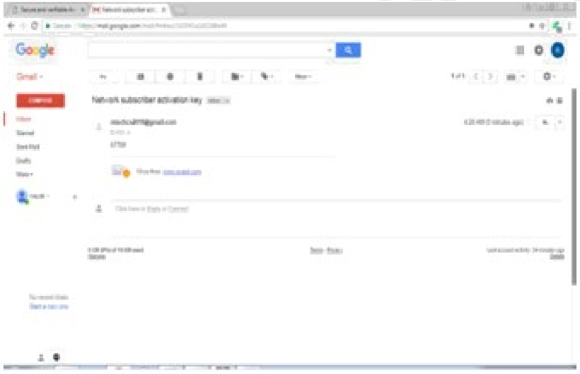
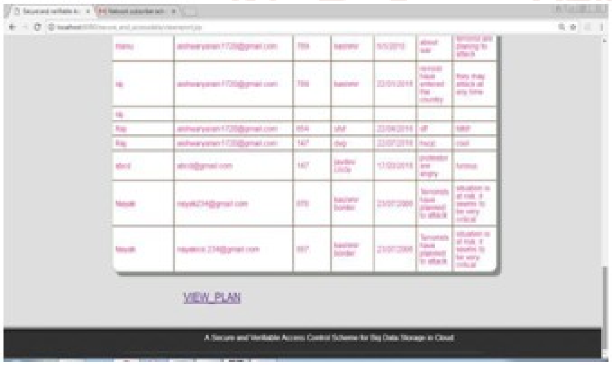


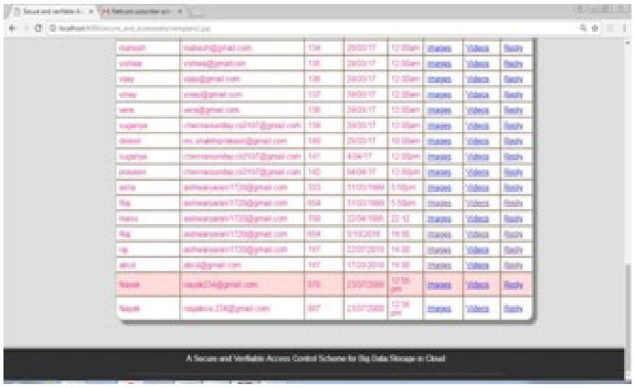
Figure 13: Screenshot of Commander’s mail-id



VIEW_PLAN

A Secure and Verifiable Access Control Scheme for Big Data Storage in Cloud

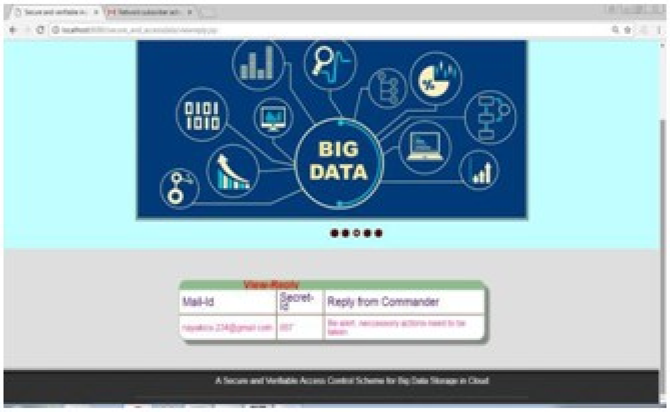
Figure 14: Screenshot of decrypted data



A Secure and Verifiable Access Control Scheme for Big Data Storage in Cloud

Figure 15: Screenshot of Reply option for commander

The figure 15 shows the screenshot of reply option for commander. On click of reply link, the commander can send reply to soldier.



View-Reply

Mail-Id	Secret-id	Reply from Commander
nayakira.234@gmail.com	897	Be alert, necessary actions need to be taken

A Secure and Verifiable Access Control Scheme for Big Data Storage in Cloud

Figure 16: Screenshot of view reply page

VIII. CONCLUSION AND FUTURE SCOPE

The projected framework was created along with an intention of giving thorough protection toward the secret data when distributed via the cloud, it regularly inclined to protection dangers by means of the interlopers with the hidden NTRU positioned encryption and decryption strategies. Evidently, it discovers a tremendous request in the section of Intelligence and digital dangers in different inward and outer resistance framework. Henceforth, the projected framework reproduces the run of the mill data distributing procedure amid the resistance work force and effectively demonstrates that the information distributed by means of the cloud is enveloped along with fundamental protection highlights and available just the approved event. The projected framework has thoroughly dissected the rightness, protection quality, and calculation multifaceted nature of the projected conspire.

In spite of the fact that the framework gives sufficient protection, however the likelihood of furious the protection stays less, the ascent in intense calculation equipment that utilization dimension processing procedures may at present have the capacity to disentangle the data effectively. Thus, a calculation that can identify the gatecrasher's action in view of authentic records would be alluring in outlook and henceforth an artificial engineering learning calculations for abnormality identification may be conveyed over the current arrangement. The outlook investigation incorporates enhancing the plan through joining limit mystery imparting to trait positioned admission manage, it includes an entrance arrangement that could put different prerequisites for a client to unscramble a sub contracted figure content statistics located at the cloud.

The future research includes improving the scheme by combining threshold secret sharing with attribute based access control, which involves an access structure that can place various requirements for a user to decrypt an outsourced cipher text data in the cloud.

IX. REFERENCES

1. Chunqiang Hu et al., “A Secure and Verifiable Access Control Scheme for Big Data Storage in Clouds” IEEE Transactions on Big data, Year: 2017, Volume: PP, Issue: 99
2. C. Hu, H. Li, Y. Huo, T. Xiang, and X. Liao, “Secure and efficient data communication protocol for wireless body area networks,” IEEE Transactions on Multi-Scale Computing Systems, vol. 2, no. 2, pp. 94–107, 2016.
3. C. Hu, X. Cheng, Z. Tian, J. Yu, K. Akkaya, and L. Sun, “An attribute based signcryption scheme to secure attribute-defined multicast communications,” in SecureComm 2015. Springer, 2015, pp. 418–435.
4. C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, “Body area network security: a fuzzy attribute-based signcryption scheme,” IEEE journal on selected areas in communications, vol. 31, no. 9, pp. 37–46, 2013.
5. V. Marx, “Biology: The big challenges of big data,” Nature, vol. 498, no. 7453, pp. 255–260, 2013.
6. C. Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen, “Securing communications between external users and wireless body area networks,” in Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy. ACM, 2013, pp. 31–36.
7. M. A. Beyer and D. Laney, “The importance of big data: a definition,” Stamford, CT: Gartner, 2012.
8. B. Waters, “Cipher text-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” Public Key Cryptography–PKC 2011, pp. 53–70, 2011.
9. J Hoffstein, “NTRU Public Key Cryptosystem–Methodology”, shodhganga.inflibnet.ac.in/ bit stream/1060 3/103254/10/10_chapter-iii.pdf.