**THE APPLICATION OF CRYPTOGRAPHY RESOURCE SYSTEM IN CLOUD COMPUTING**

**ABSTRACT:**

* Due to the complexity and volume, outsourcing cipher texts to a cloud is deemed to be one of the most effective approaches for big data storage and access.
* Nevertheless, verifying the access legitimacy of a user and securely updating a cipher text in the cloud based on a new access policy designated by the data owner are two critical challenges to make cloud-based big data storage practical and effective.
* Traditional approaches either completely ignore the issue of access policy update or delegate the update to a third party authority; but in practice, access policy update is important for enhancing security and dealing with the dynamism caused by user join and leave activities.
* In this paper, we propose a secure and verifiable access control scheme based on the NTRU cryptosystem for big data storage in clouds.
* We first propose a new NTRU decryption algorithm to overcome the decryption failures of the original NTRU, and then detail our scheme and analyze its correctness, security strengths, and computational efficiency.
* Our scheme allows the cloud server to efficiently update the cipher text when a new access policy is specified by the data owner, who is also able to validate the update to counter against cheating behaviors of the cloud. It also enables (i) the data owner and eligible users to effectively verify the legitimacy of a user for accessing the data, and (ii) a user to validate the information provided by other users for correct plaintext recovery.
* Rigorous analysis indicates that our scheme can prevent eligible users from cheating and resist various attacks such as the collusion attack.

**INTRODUCTION:**

BIG data is a high volume, and/or high velocity, high variety information asset, which requires new forms of processing to enable enhanced decision making, insight discovery, and process optimization. Due to its complexity and large volume, managing big data using on hand database management tools is difficult. An effective solution is to outsource the data to a cloud server that has the capabilities of storing big data and processing users’ access requests in an efficient manner. For example in ehealth applications, the genome information should be securely stored in an e-health cloud as a single sequenced human genome is around 140 gigabytes in size. However, when a data owner outsources its data to a cloud, sensitive information may be disclosed because the cloud server is not trusted; therefore typically the ciphertext of the data is stored in the could. But how to update the ciphertext stored in a cloud when a new access policy is designated by the data owner and how to verify the legitimacy of a user who intends to access the data are still of great concerns.

**SCOPE OF THE PROJECT:**

An improved NTRU cryptosystem to overcome the decryption failures of the original NTRU. Then we design a secure and verifiable scheme based on the improved NTRU and secret sharing for big data storage. The cloud server can directly update the stored ciphertext without decryption based on the new access policy specified by the data owner, who is able to validate the update at the cloud. The proposed scheme can verify the shared secret information to prevent users from cheating and can counter various attacks such as the collusion attack. It is also deemed to be secure with respect to quantum computing attacks due to NTRU.

**LITERATURE SURVEY:**

**Title:**Securing Communications Between External Users and Wireless Body Area Networks

**Author:**Chunqiang Hu

**Year:**2013

**DESCRIPTION:**

Wireless Body Area Networks (BANs) are expected to play a crucial role in patient-health monitoring in the near future. Establishing secure communications between BAN sensors and external users is key to addressing the prevalent security and privacy concerns. In this paper, we propose the primitive functions to implement a secret-sharing based Ciphertext-Policy Attribute-Based Encryption (CP\_ABE) scheme, which encrypts the data based on an access structure specified by the data source. We also design two protocols to securely retrieve the sensitive patient data from a BAN and instruct the sensors in a BAN. Our analysis indicates that the proposed scheme is feasible, can provide message authenticity, and can counter possible major attacks such as collusion attacks and battery-draining attacks.

**Title:**Secure and Efficient data communication protocol for Wireless Body Area Networks

**Author:**Chunqiang Hu,

**Year:**2016

**DESCRIPTION:**

Wireless Body Area Networks (WBANs) are expected to play a major role in the field of patient-health monitoring in the near future, which gains tremendous attention amongst researchers in recent years. One of the challenges is to establish a secure communication architecture between sensors and users, whilst addressing the prevalent security and privacy concerns.In this paper, we propose a communication architecture for BANs, and design a scheme to secure the data communications between implanted /wearable sensors and the data sink/data consumers (doctors or nurse) by employing Ciphertext-Policy Attribute Based Encryption (CP ABE) [1] and signature to store the data in ciphertext format at the data sink, hence ensuring data security. Our scheme achieves a role-based access control by employing an access control tree defined by the attributes of the data. We also design two protocols to securely retrieve the sensitive data from a BAN and instruct the sensors in a BAN. We analyze the proposed scheme, and argue that it provides message authenticity and collusion resistance, and is efficient and feasible. We also evaluate its performance in terms of energy consumption and communication/computation overhead.

**Title:**Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data

**Author:**VipulGoyal

**Year:**2006

**DESCRIPTION:**  
As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KPABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. We demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

**Title:**Body Area Network Security: A Fuzzy Attribute-Based Signcryption Scheme

**Author:**Nan Zhang,

**Year:**2012

**DESCRIPTION:**

Body Area Networks (BANs) are expected to play a major role in the field of patient-health monitoring in the near future. While it is vital to support secure BAN access to address the obvious safety and privacy concerns, it is equally important to maintain the elasticity of such security measures. For example, elasticity is required to ensure that first-aid personnel have access to critical information stored in a BAN in emergent situations. The inherent tradeoff between security and elasticity calls for the design of novel security mechanisms for BANs. In this paper, we develop the Fuzzy Attribute-Based Signcryption (FABSC), a novel security mechanism that makes a proper tradeoff between security and elasticity. FABSC leverages fuzzy Attribute-based encryption to enable data encryption, access control, and digital signature for a patient’s medical information in a BAN. It combines digital signatures and encryption, and provides confidentiality, authenticity, unforgeability, and collusion resistance. We theoretically prove that FABSC is efficient and feasible. We also analyze its security level in practical BANs.

**Title:**An efficient threshold verifiable multi-secret sharing

**Author:**MassoudHadianDehkordi

**Year:**2007

**DESCRIPTION:**

In order to keep the secret efficiently and safely, in 1979, Shamir andBlakley first developed the concepts of the secret sharing (SS) scheme. The former is based on the Lagrange interpolating polynomial, while the latter is based on the linear projective geometry. In these secret sharing there are several problems as follows: (1) In every secret sharing process only one secret can be shared; (2) These secret sharing are the one-time-use scheme, in other words once the secret has been reconstructed, dealer must redistribute a fresh shadow over a secure channel to every participant; (3) In both of them it is supposed that the dealer and participants are honest but in fact it is impossible in the real word and a dishonest dealer may distribute a fake shadow to a certain participant or a malicious participant may provide a fake share to other participants.

**Title:**A verifiable multi-secret sharing scheme based on cellular automata

**Author:**Eslami, J. ZarepourAhmadabadi

**Year:**2010

**DESCRIPTION:**

Cryptographic procedures to share a secret K among a set of participants P such that only qualified subsets of P can recover the secret are known as secret sharing schemes Such schemes were independently introduced by Shamir and Blakley and their original motivation was to safeguard cryptographic keys from loss. In recent times, secret sharing schemes have found applications in diverse areas such as access control systems, e-voting schemes and digital cash protocols, to name a few. An important example in this regard is the (t,n)-threshold secret sharing scheme in which jPj ¼ n and qualified subsets consist of all sets of participants with cardinality at least t. There is a mutually trusted party (called the dealer) who distributes the shares among n participants in such a way that any t of them can recover the original secret, but any group knowing only t 1 or fewer shares can not. If knowing t 1 (or fewer) shares provides no information about the secret, the scheme is called perfect. Shamir’s scheme, which is based on polynomial interpolation, and Blakley’s scheme, based on the intersection of affine hyperplanes, are examples of (t,n)-threshold schemes. However, one can distinguish the following drawbacks in these schemes:

**Title:**New efficient and practical verifiable multi-secret sharing schemes

**Author:**MassoudHadianDehkordi

\**Year:**2007

**DESCRIPTION:**

Secret sharing plays an important role in protecting secret information from becoming lost, destroyed, or falling into the wrong hands [3–18]. It has been an interesting branch of modern cryptography [20–22,24–26]. In verifiable multi-secret sharing, there are multiple secrets to be shared during a secret sharing process, and any cheating by a dealer or by participants can be detected [8–10,15,22,26]. In 2005, Shao and Cao (SC) [22] proposed an efficient verifiable multi-secret sharing based on Yang et al.’s (YCH) and Feldman’s schemes [25,10]. In the SC scheme, the dealer, distributes each secret shadow si to each participant Mi over a secure channel. In 2006, Zhao et al. (ZZZ) [26] proposed a practical verifiable multi-secret sharing based on YCH and Hwang–Chang (HC) schemes [25,15]. The verification phase of the ZZZ scheme is the same as that of the HC scheme. The RSA cryptosystem and a Diffie–Helman key agreement method [23] are employed in the HC and ZZZ schemes. Hence, a secure channel is unnecessary. This property is of particular value to the system which is unlikely to exist in the security channel. In addition, each participant chooses his secret shadow by himself. This also cuts the dealer’s amount of computing.

**Title:**secret image sharing based on chaotic map and chinese remainder theorem

**Author:**XIAOFENG LIAO

**Year:**2011

**DESCRIPTION:**

Secret sharing is an efficient method for transmitting the image securely. This paper proposes an efficient secret sharing scheme for secret image. The protocol allows each participant to share a secret gray image with the rest of participants. In our scheme, a secret digital image is divided into n pieces, which are further distributed into n participants. The secret digital image can be reconstructed if and only if r or more legal participants cooperate together. These schemes have no pixel expansion. It is general in nature and can be applied on any image size. The proposed scheme is based on the chaotic map and the Chinese Remainder theorem. The security of the scheme is analyzed and the protocol is proven to be secure and be able to resist statistic and exhaustive attacks.

**MODULE:**

* **USER INTERFACE DESIGN**
* **OWNER UPLOAD DETAILSANDSEND TO CUSTOMS**
* **CUSTOM’S USER CHECK DETAILS**
* **REQUEST SEND TO OWNER**
* **CUSTOM’S SEND TO CUSTOMER**
* **CUSTOMER REQUEST SEND TO OWNER**

**DESCRIPTION:**

* **User Interface Design**

To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. . Logging in is usually used to enter a specific page

* **Owner Upload Details And Send To Custom’s**

Owner choose the product and details example product id, product name, cost, piece, custom’s name, company name, net weight so all details and high level security of encryption and key also developed, owner send to custom’s side.

* **Custom’s User Check Details**

Custom’s user one data receive so check the details, the details also encryption format so all information is print \*\*\*\*\* only

* **REQUEST SEND TO OWNER**

Custom’s User view original data means send request to data owner. The data owner monitoring the file and accept.

* Custom’s Send To Customer

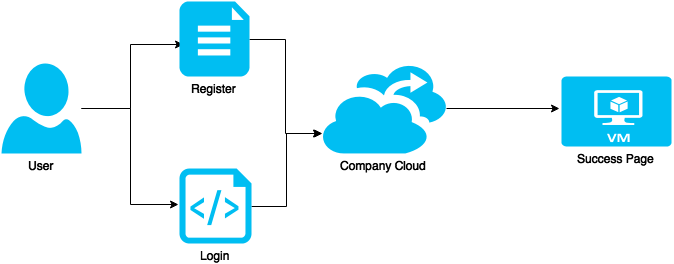
Custom’s user view the original content and download the product. The custom’s user send to customer

* Customer Request Send To Owner

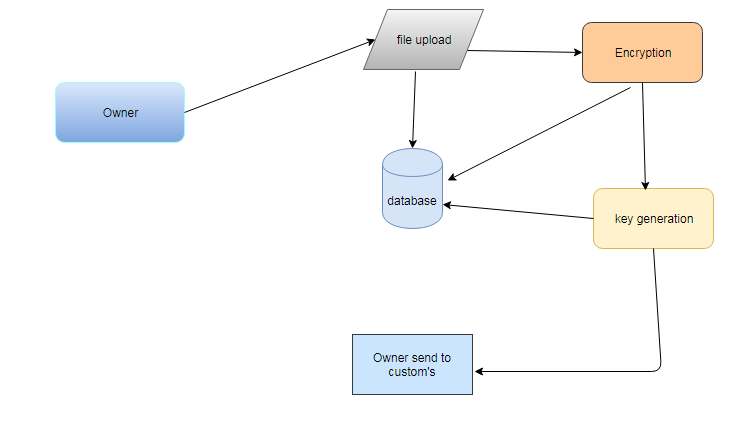
Customer view the message only star format so customer send the request so the owner vie the inbox and accept the query, customer view the original data.

**MODULE DIAGRAM:**

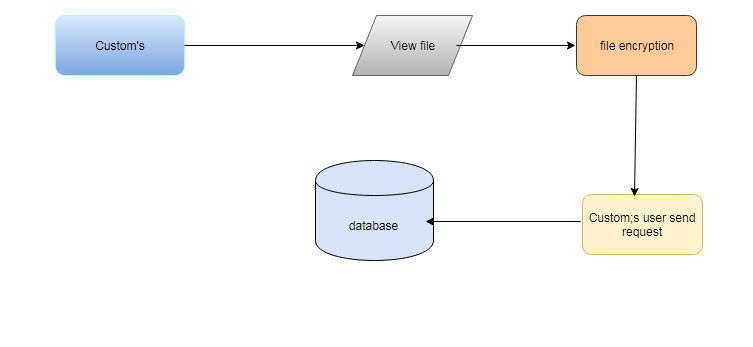
* **User Interface Design**

****

* **Owner Upload Details And Send To Custom’s**

****

* **Custom’s User Check Details**



* **REQUEST SEND TO OWNER**

Custom’s user

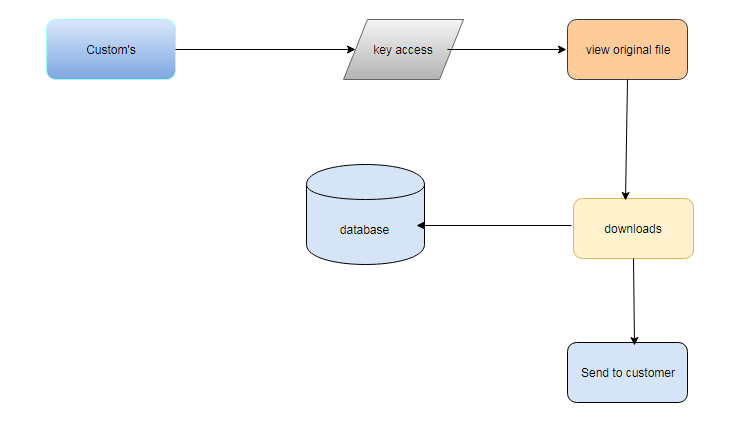
Key request

Monitoring request

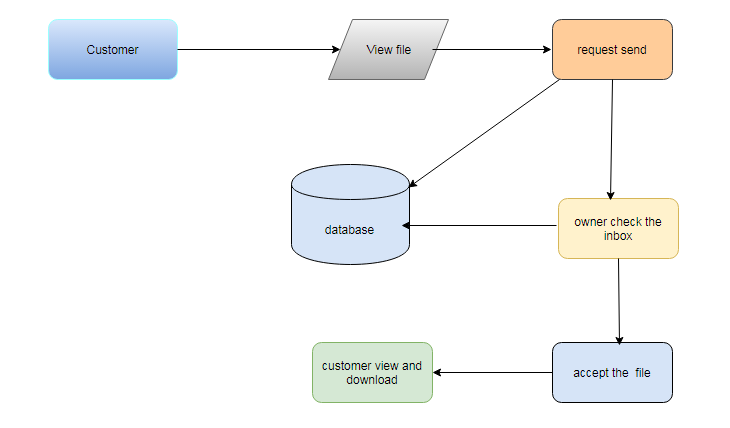
Owner check inbox

Key accept

* Custom’s Send To Customer



* Customer Request Send To Owner



**SYSTEM TECHNIQUE:**

An efficient and verifiable method to update the cipher text stored in clouds without increasing any risk when the access policy is dynamically changed by the data owner for various reasons. The verifying the shared secret information to prevent users from cheating and can counter various attacks such as the collusion attack.

NTRU is a patented and open source public-key cryptosystem that uses latticebased cryptography to encrypt and decrypt data. It consists of two algorithms: NTRU Decrypt, which is used for Decryption, and NTRUSign, which is used for digital signatures.

**SYSTEM REQUIREMENTS**

**HARDWARE**

PROCESSOR : DUALCORE 2 DUO.

RAM : 4GB DD RAM

MONITOR : 15” COLOR

HARD DISK : 250 GB

**SOFTWARE**

Front End : JAVA (J2EE, SERVLETS, JSP)

Back End : MY SQL 5.5

Operating System : Windows 07

IDE : Eclipse

**Use Case Diagram:**

owner

custom's

customer

register

login

upload

request

download file

encryption file

send

response

**EXPLANATION:**

The main purpose of a use case diagram is to show what system functions are performed foruser can login and company also login. Owner choose the product and details example product id, product name, cost, piece, custom’s name, company name, net weight so all details and high level security of encryption and key also developed, owner send to custom’s side. Custom’s user one data receive so check the details, the details also encryption format so all information is print \*\*\*\*\* only.Custom’s user view the original content and download the product. The custom’s user send to customer.Customer view the message only star format so customer send the request so the owner vie the inbox and accept the query, customer view the original data.

**Class Diagram:**

Owner



Register



Login



Upload product



key



encrypt



allow



accept

Custom’s



Register



Login



View

\



File encrypted



Request send

Customer



Login



Request send

View original file

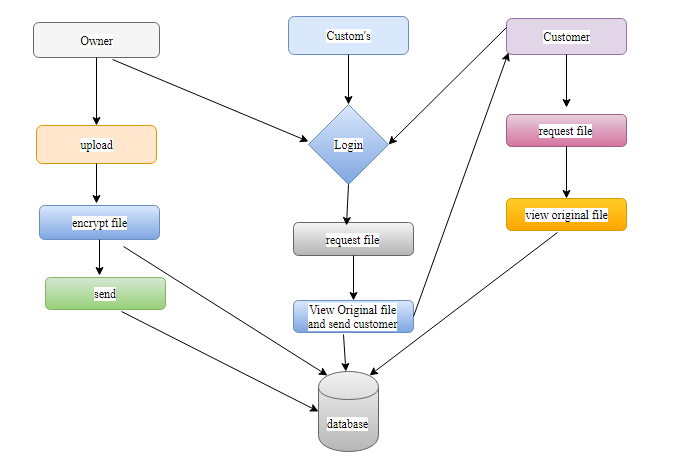
Database

**EXPLANATION:**

The class diagram is the main building block of object oriented modeling. It is used both for general conceptual modeling of the systematic of the application, and for detailed modeling translating the models into programming code in the Diagram we are user can login and company also login. . Owner choose the product and details example product id, product name, cost, piece, custom’s name, company name, net weight so all details and high level security of encryption and key also developed, owner send to custom’s side. Custom’s user one data receive so check the details, the details also encryption format so all information is print \*\*\*\*\* only.Custom’s user view the original content and download the product. The custom’s user send to customer.Customer view the message only star format so customer send the request so the owner vie the inbox and accept the query, customer view the original data.

.

**Object Diagram:**

****

**EXPLANATION:**

Object diagram we are telling about the flow of objects how the process is running. In the above digram tells about the flow of objects between the classes.In the Diagram for user can login and company also login. . Owner choose the product and details example product id, product name, cost, piece, custom’s name, company name, net weight so all details and high level security of encryption and key also developed, owner send to custom’s side. Custom’s user one data receive so check the details, the details also encryption format so all information is print \*\*\*\*\* only.Custom’s user view the original content and download the product. The custom’s user send to customer.Customer view the message only star format so customer send the request so the owner vie the inbox and accept the query, customer view the original data.

**State Diagram:**

Owner

Customs

Customer

Login

Upload

Encrypted

Key

Decrypt

**EXPLANATION:**

State diagrams require that the system described is composed of a finite number of states; sometimes, this is indeed the case, while at other times this is a reasonable abstraction. Many forms of state diagrams exist, which differ slightly and have different semantics.In the Diagram for is to expose what device capabilities are performed for user can login and company also login. . Owner choose the product and details example product id, product name, cost, piece, custom’s name, company name, net weight so all details and high level security of encryption and key also developed, owner send to custom’s side. Custom’s user one data receive so check the details, the details also encryption format so all information is print \*\*\*\*\* only.Custom’s user view the original content and download the product. The custom’s user send to customer.Customer view the message only star format so customer send the request so the owner vie the inbox and accept the query, customer view the original data.

**Activity Diagram:**

Owner

Customs

Customer

Register

Login

Key

Encrypt

View

Original file

Upload

**EXPLANATION:**

In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control. In the Diagram we showfor user can login and company also login. The person are upload file and view the files. The file are two type are store in public and private. The file also download the file. User And Company store the file for public. The user store the private file it will be show only that user and organization. The file also view online and edit the file and store the file in cloud. The user only can edit the file for the user can view the file.

**Sequence Diagram:**

Owner

Customs

Customer

Cloud

Register For Company

Register

Login

Login

Upload File

Upload

Encrypt View

View

View File

Search

Public View And Private View file

Search File

Monitor user

**EXPLANATION:**

In our sequence diagram specifying processes operate with one another and in order. In our sequence diagram for is to expose what device capabilities are performed for user can login and company also login. . Owner choose the product and details example product id, product name, cost, piece, custom’s name, company name, net weight so all details and high level security of encryption and key also developed, owner send to custom’s side. Custom’s user one data receive so check the details, the details also encryption format so all information is print \*\*\*\*\* only.Custom’s user view the original content and download the product. The custom’s user send to customer.Customer view the message only star format so customer send the request so the owner vie the inbox and accept the query, customer view the original data.

**Collaboration Diagram**:

Customs

Owner

Customer

Cloud

1: Register

2: Login

3: Register For Company Cloud

4: Login

5: Upload File

6: Uplaod

7: Encrypt View

8: View

9: Request File

10: Key

11: Response file key access

12: Request File

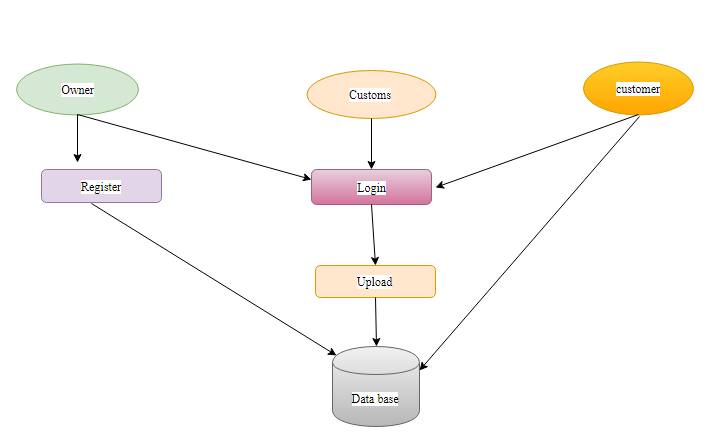
13: Monitor user

**EXPLANATION:**

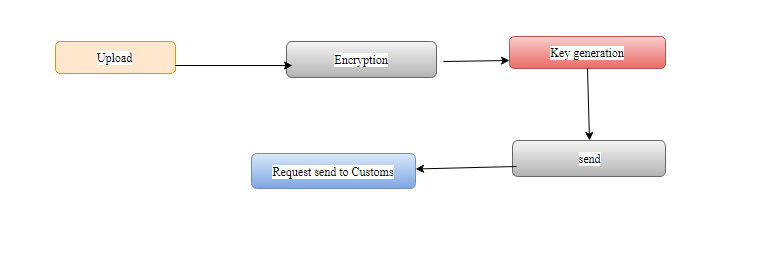
A collaboration diagram describes interactions among objects in terms of sequenced messages. Collaboration diagrams represent a combination of information taken from class, sequence, and use case diagrams describing both the static structure and dynamic behavior of a system.In the Diagram we show for user can login and company also login. . Owner choose the product and details example product id, product name, cost, piece, custom’s name, company name, net weight so all details and high level security of encryption and key also developed, owner send to custom’s side. Custom’s user one data receive so check the details, the details also encryption format so all information is print \*\*\*\*\* only.Custom’s user view the original content and download the product. The custom’s user send to customer.Customer view the message only star format so customer send the request so the owner vie the inbox and accept the query, customer view the original data.

**Data Flow Diagram:**

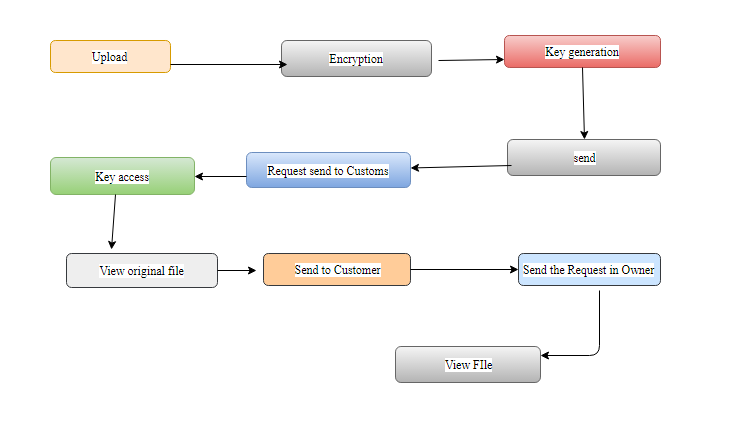
Level 0:



Level 1:



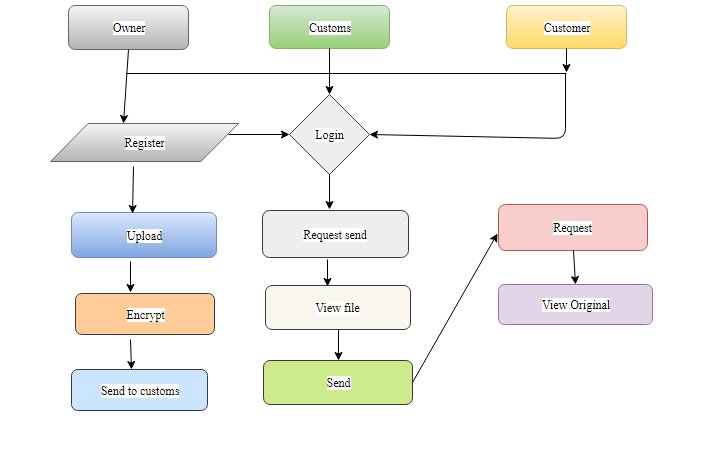
Level 2:



**EXPLANATION:**

It does not show information about the timing of processes, or information about whether processes will operate in sequence or in parallel. In the DFDs the level zero process is based on the login validations. . Owner choose the product and details example product id, product name, cost, piece, custom’s name, company name, net weight so all details and high level security of encryption and key also developed, owner send to custom’s side. Custom’s user one data receive so check the details, the details also encryption format so all information is print \*\*\*\*\* only.Custom’s user view the original content and download the product. The custom’s user send to customer.Customer view the message only star format so customer send the request so the owner vie the inbox and accept the query, customer view the original data.

**E-R Diagram:**



**EXPLANATION:**

Entity-Relationship Model (ERM) is an abstract and conceptual representation of data. Entity-relationship modeling is a database modeling method, used to produce a type of conceptual schema or semantic data model of a system, often a relational database.In the Diagram we showfor user can login and company also login. . Owner choose the product and details example product id, product name, cost, piece, custom’s name, company name, net weight so all details and high level security of encryption and key also developed, owner send to custom’s side. Custom’s user one data receive so check the details, the details also encryption format so all information is print \*\*\*\*\* only.Custom’s user view the original content and download the product. The custom’s user sends to customer.Customer view the message only star format so customer send the request so the owner vie the inbox and accept the query, customer view the original data.

**Component Diagram:**

Owner

Customs

Customer

Register

Login

Encrypt

Upload

Request Send

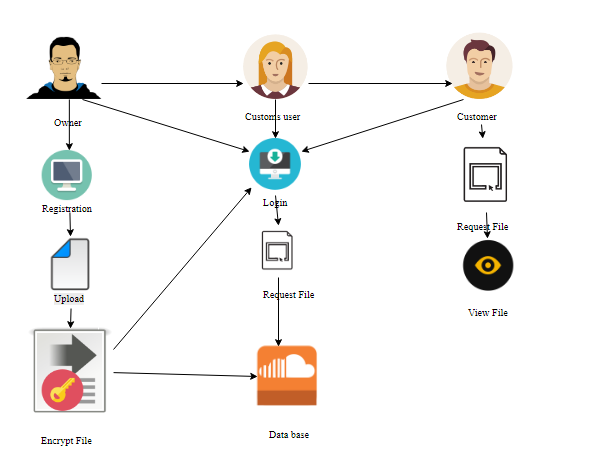
View file

Key generation

**EXPLANATION:**

In the Unified Modeling Language, a component diagram depicts how components are wired together to form larger components and they are used to illustrate the structure of arbitrarily complex systems.In the Diagram we show for is to expose what device capabilities are performed for user can login and company also login. Owner choose the product and details example product id, product name, cost, piece, custom’s name, company name, net weight so all details and high level security of encryption and key also developed, owner send to custom’s side. Custom’s user one data receive so check the details, the details also encryption format so all information is print \*\*\*\*\* only.Custom’s user view the original content and download the product. The custom’s user sends to customer.Customer view the message only star format so customer send the request so the owner vie the inbox and accept the query, customer view the original data.

**System Architecture:**



**Proposed System Model Explanation**

Owner choose the product and details example product id, product name, cost, piece, custom’s name, company name, net weight so all details and high level security of encryption and key also developed, owner send to custom’s side. Custom’s user one data receive so check the details, the details also encryption format so all information is print \*\*\*\*\* only.Custom’s user view the original content and download the product. The custom’s user sends to customer.Customer view the message only star format so customer send the request so the owner vie the inbox and accept the query, customer view the original data.An efficient and verifiable method to update the cipher text stored in clouds without increasing any risk when the access policy is dynamically changed by the data owner for various reasons. The verifying the shared secret information to prevent users from cheating and can counter various attacks such as the collusion attack.

NTRU is a patented and open source public-key cryptosystem that uses latticebased cryptography to encrypt and decrypt data. It consists of two algorithms: NTRU Decrypt, which is used for Decryption, and NTRUSign, which is used for digital signatures.

**ADVANTAGES:**

* The data owner and eligible users to effectively verify the legitimacy of a user for accessing the data.
* To upload their endless data.
* Corresponding computations to a third party

**FUTURE ENHANCEMENT:**

* The security problems when a data owner outsources its data to multicloud servers and consider an attribute-based access structure that can be dynamically updated, which is more applicable for practical scenarios in big data storage.Designing a secure, privacy preserving, and practical scheme for big data storage in a cloud.

**CONCLUSION:**

In this paper, we first propose an improved NTRU cryptosystem to overcome the decryption failures of the original NTRU and then present a secure and verifiable access control scheme based on the improved NTRU to protect the outsourced big data stored in a cloud. Our scheme allows the data owner to dynamically update the data access policy and the cloud server to successfully update the corresponding outsourced ciphertext to enable efficient access control over the big data in the cloud. It also provides a verification process for a user to validate its legitimacy of accessing the data to both the data owner and t􀀀1 other legitimate users and the correctness of the information provided by the t1 other users for plaintext recovery. The security of our proposed scheme is guaranteed by those of the NTRU cryptosystem and the (t; n)-threshold secret sharing. We have rigorously analyzed the correctness, security strength, and computational complexity of our proposed scheme. Designing a secure, privacy preserving, and practical scheme for big data storage in a cloud is an extremely challenging problem. In our future research, we will further improve our scheme by combining the (t; n)-threshold secret sharing with attributebased access control, which involves an access structure that can place various requirements for a user to decrypt an outsourced ciphertext data in the cloud. Meanwhile, we will investigate the security problems when a data owner outsources its data to multicloud servers and consider an attribute-based access structure that can be dynamically updated, which is more applicable for practical scenarios in big data storage.

**REFERENCES**

[1] M. A. Beyer and D. Laney, “The importance of big data: a definition,” Stamford, CT: Gartner, 2012.

[2] V. Marx, “Biology: The big challenges of big data,” Nature, vol. 498, no. 7453, pp. 255–260, 2013.

[3] G. P. Consortium et al., “A map of human genome variation from population-scale sequencing,” Nature, vol. 467, no. 7319, pp. 1061–1073, 2010.

[4] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” Advances in Cryptology–EUROCRYPT 2005, pp. 457–473, 2005.

[5] 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.

[6] 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.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 89–98.

[8] sB. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” Public Key Cryptography– PKC 2011, pp. 53–70, 2011.

[9] 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.

[10] A. Lewko and B. Waters, “Decentralizing attribute-based encryption,” Advances in Cryptology–EUROCRYPT 2011, pp. 568–588, 2011.

[11] C. Hu, X. Cheng, Z. Tian, J. Yu, K. Akkaya, and L. Sun, “An attributebasedsigncryption scheme to secure attribute-defined multicast communications,” in SecureComm 2015. Springer, 2015, pp. 418–435.

[12] A. Shamir, “Identity-based cryptosystems and signature schemes,” in Advances in cryptology. Springer, 1985, pp. 47–53.

[13] M. Dehkordi and S. Mashhadi, “An efficient threshold verifiable multisecret sharing,” Computer Standards & Interfaces, vol. 30, no. 3, pp. 187–190, 2008.

[14] Z. Eslami and J. Z. Ahmadabadi, “A verifiable multi-secret sharing scheme based on cellular automata,” Information Sciences, vol. 180, no. 15, pp. 2889–2894, 2010.

[15] M. H. Dehkordi and S. Mashhadi, “New efficient and practical verifiable multi-secret sharing schemes,” Information Sciences, vol. 178, no. 9, pp. 2262–2274, 2008.