MODIFIED HOMOMORPHIC ENCRYPTION ALGORITHM TO SECURE DATA IN CLOUD COMPUTING

Dissertation submitted in fulfilment of the requirements for the Degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

By

JASLEEN SAINI

11503027

Supervisor

ROSHAN SHRIVASTAVA

(Asst. Professor)

School of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab (India)

May, 2017

TOPIC APPROVAL PERFORMA

School of Computer Science and Engineering

Program : P172::M.Tech. (Computer Science and Engineering) [Full Time]

COURSE CODE : CSE546 **REGULAR/BACKLOG :** Regular **GROUP NUMBER :** CSERGD0273

Supervisor Name : Roshan Srivastava **UID :** 16876 **Designation :** Assistant Professor

Qualification : _____ **Research Experience :** _____

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Jasleen Saini	11503027	2015	K1519	9914355810

SPECIALIZATION AREA : Networking and Security **Supervisor Signature:** _____

PROPOSED TOPIC : Cloud Computing Security

Qualitative Assessment of Proposed Topic by PAC		
Sr.No.	**Parameter**	**Rating (out of 10)**
1	Project Novelty: Potential of the project to create new knowledge	6.80
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	6.80
3	Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program.	7.20
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	7.40
5	Social Applicability: Project work intends to solve a practical problem.	7.20
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	7.60

PAC Committee Members		
PAC Member 1 Name: Prateek Agrawal	UID: 13714	Recommended (Y/N): Yes
PAC Member 2 Name: Pushpendra Kumar Pateriya	UID: 14623	Recommended (Y/N): Yes
PAC Member 3 Name: Deepak Prashar	UID: 13897	Recommended (Y/N): Yes
PAC Member 4 Name: Kewal Krishan	UID: 11179	Recommended (Y/N): Yes
PAC Member 5 Name: Anupinder Singh	UID: 19385	Recommended (Y/N): NA
DAA Nominee Name: Kanwar Preet Singh	UID: 15367	Recommended (Y/N): Yes

Final Topic Approved by PAC: **Modified Homomorphic Encryption Algorithm to secure data in cloud computing**

Overall Remarks: Approved (with major changes)

PAC CHAIRPERSON Name: 11011::Dr. Rajeev Sobti **Approval Date:** 22 Nov 2016

ABSTRACT

Cloud Computing offers the best platform in which data is stored and also the data is shared from one network to another. Some organizations have their own cloud to store their information. But there are some security issues in cloud and hence, Attribute-based encryption is becoming a favourable to guarantee data security in cloud computing. In this the set of attributes are used for encryption, the person who has correct set of attributes, can only decrypt the data. The homomorphic encryption is used in which mathematical operations are done on encrypted data without compromising the encryption. Homomorphic operation is done on the cipher text to make the encryption difficult so that any random third party cannot access the data to be transferred on the network. By using this attribute based algorithm having homomorphic encryption, the security aspect and the performance of the algorithm is analyzed. In modified homomorphic encryption both additive and multiplicative operations along with diffie hellman key exchange in which prime numbers are selected which is better than homomorphic encryption. This makes the encryption more difficult to dycrypt by the attackers.

DECLARATION STATEMENT

I hereby declare that the research work reported in the dissertation entitled **"**MODIFIED HOMOMORPHIC ENCRYPTION ALGORITHM TO SECURE DATA IN CLOUD COMPUTING" in partial fulfilment of the requirement for the award of Degree for Master of Technology in Computer Science and Engineering at Lovely Professional University, Phagwara, Punjab is an authentic work carried out under supervision of my research supervisor Mr. Roshan Shrivastava. I have not submitted this work elsewhere for any degree or diploma.

I understand that the work presented herewith is in direct compliance with Lovely Professional University's Policy on plagiarism, intellectual property rights, and highest standards of moral and ethical conduct. Therefore, to the best of my knowledge, the content of this dissertation represents authentic and honest research effort conducted, in its entirety, by me. I am fully responsible for the contents of my dissertation work.

JASLEEN SAINI

11503027

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the M.Tech Dissertation entitled "MODIFIED HOMOMORPHIC ENCRYPTION ALGORITHM TO SECURE DATA IN CLOUD COMPUTING**"**, submitted by **Jasleen Saini** at **Lovely Professional University; Phagwara, India** is a bonafide record of her original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

Roshan Shrivastava

Date:

Counter Signed by:

1) **Concerned HOD:**
   HoD's Signature: _____

   HoD Name: _____

   Date: _____

2) **Neutral Examiners:**

   External Examiner

   Signature: _____

   Name: _____

   Affiliation: _____

   Date: _____

   Internal Examiner

   Signature: _____

   Name: _____

   Date: _____

ACKNOWLEDGEMENT

I would like to express profound gratitude to my guide **Roshan Srivastava, Asst. Prof, School of Computer Science Engineering** for his invaluable support, encouragement, supervision and useful suggestions throughout my work. His moral support and continuous guidance motivated me to complete my work successfully.

I am grateful for the cooperation and encouragement from the faculty members of Computer Science Department. Their regular suggestions made my work easy and proficient.

Last but not the least, I am thankful and indebted to all those who helped me directly or indirectly in completion of my Dissertation-I report.

Jasleen Saini

11503027

TABLE OF COMPONENT

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 Cloud Computing

Cloud computing is a type of computing which is in the internet in which data is shared using different processing resources and share it to the other users on demand. It is architecture which is when demanded by the user access of resources which are used as a shared pool for e.g., storage, computer networks, applications, servers and services that can be provided very fast and provided with minimum organized effort. [17].The solution for storage in Cloud computing provide various users and various enterprises having different capabilities to process and store their information in some another databases that can be present at remote areas from the user and can be in another city or in different country in the world. Cloud computing is basically a resource sharing computing to achieve consistency and to increase the level of production[21].

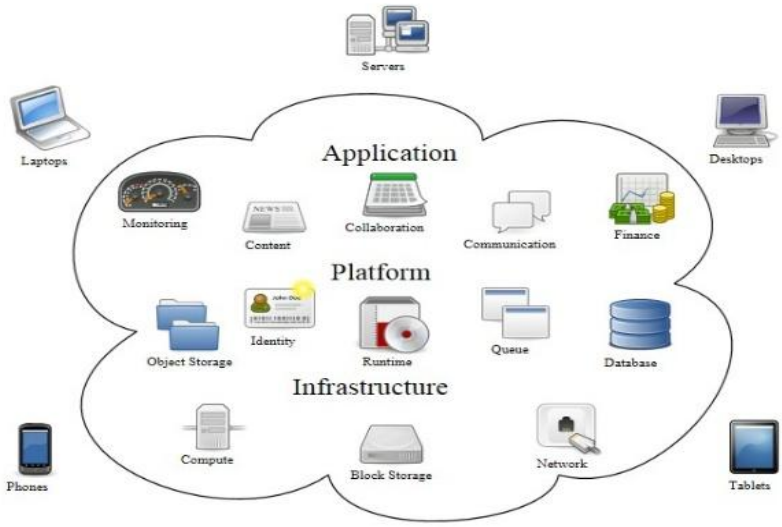

Figure 1.1: Service categories in a cloud with various components implemented at various levels[17]

The National Institute of Standards and Technology's define for cloud computing provides "five important characteristics":

On-demand self-service: A user alone can manage the capabilities of computing, for example server time and storage in network, which can be easily available without communicate with the service providers.

Broad network access: As the network is too large, so the user can take any resource at any time without taking any permission to anyone. Even the person can access the network at any time at any place.

Resource pooling: The resources are available on the network for the users so that they can use it whenever there is some requirement. The pool of resources is present in all servers so that the user can use it for their own purpose.

Rapid elasticity: The capabilities are provided in order to make the provision of resources fast to the user. If the provision is fast then the elasticity also increases. So, the resources are always available on the network and can be used by the users.

Measured service: Cloud computing controls the data stored in the networked and all the services are measured for e.g., storage, bandwidth, processing, user accounts. Resources which are in use are monitored and controlled which provides reliability for both the consumer and provider of the application to be utilized[29].

There are some common reasons that the organizations are moving for the services of cloud computing:

1. Cost: Cloud computing completely removes the price of assets of purchasing the software and the hardware and setting up the data center and moving on-site data center which are the servers, and the power and cooling round-the-clock electricity and the experts of IT for controlling the infrastructure.

2. Speed: Most of the services of cloud are provides when in demand, so even heavy amount of resources can be provided within second, with minimum of clicks, provides business a flexibility and easy for the business.

3. Global scale: The advantages of cloud services that includes the ability of elasticity for scaling. According to the cloud, it delivers the sufficient amount of resources for IT department for example, storage, power, data transfer, when it is required and from the correct and particular location.

4. Productivity: Some data centers requires the hardware set up and software requirements are also these and other IT time consuming techniques. Cloud computing removes these time consuming tasks and helps IT organizations to do the work fast as much as possible. Due to this the productivity increases.

5. Performance: The most important and advantageous services of cloud are running to secure the data centers on the network worldwide. These are continuously upgraded

to make it fast and error free. It decreases the network latency and there is large scaling of cost. Hence, it increases the performance of the cloud computing.

6. Reliability: Cloud computing provides the recovery of the data and also the data is backed up. It makes the business easy and hence the different organizations will use the cloud with a limited cost. With the cloud, the organizations are reliable with their computing[28].

To deploy the resources of cloud computing in the network, which are of three different types: public cloud, private cloud and hybrid cloud[22].

Public cloud: The public clouds are managed and maintained by another party cloud service provider, that distributes the resources for computing like storage on the internet and the servers for transferring the data. There is an example for the public cloud which is Microsoft Azure., All the software, hardware, and other infrastructure is managed and controlled by the provider of cloud in a public cloud. The services can be controlled and manage the subject by having a web browser.

Private cloud: A Private cloud is used by the organization for their own use. The data centers are owned by the organization in order to store their data. These private clouds are used for the personal use in which the organizations store their data. These clouds are not shared any other organization or any other third party.

Hybrid cloud: Hybrid cloud is the joining of the public and the private cloud. It adopts the benefits of both the clouds. The hybrid cloud provides the flexibility and many deployment options as there are the facilities of both the private cloud and public cloud. So, this is the major advantage of using the hybrid cloud.

1.2 Cloud Computing Security

Physical security: Cloud service providers provide the reliability physically for the IT hardware like cables, servers, routers, etc. in opposition for the unauthorized access, theft, fires, interference, floods etc. and make sure about the essential supplies such as electricity are well made sufficiently to minimize the disturbance possibility[18]. This can be acquired by providing cloud applications, constructed, managed, designed, monitored and maintained by the data centers.

Personnel security: Many concerns for information security are related to the IT and other consultants linked with cloud services are easily handled through pre-

employment and post-employment activities such as security recruits for screening potential, security awareness and training programs, intense.

Privacy: Providers make sure that all important data such as credit card numbers are covered and encrypted and only authorized users have access for the use of the data. Moreover, digital products and other things must be protected with data that the provider accumulate or produces the customer activities in the cloud[23].

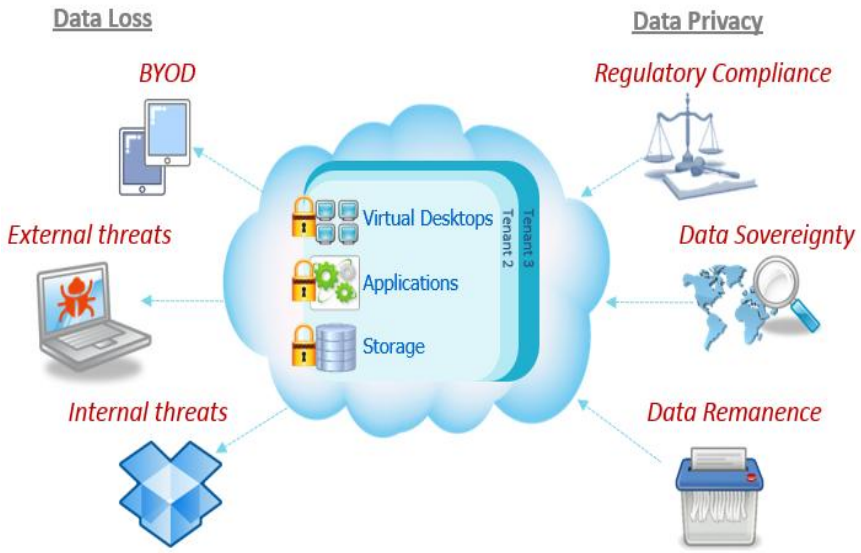

Figure 1.2: Securing cloud data[32]

There are various security hazards related with data applications of the cloud, also taking old security threats, for example denial of service attacks, network eavesdropping, and illegal invasion, but also involves particular vulnerability of cloud computing, for example side virtualization vulnerabilities, channel attacks, and misuse of cloud services. Following security requirements are there to reduce the threats that are necessary in a cloud information service.

Data Confidentiality: There is a method of Data confidentiality that the data material is not given to anyone or disclosed to any unauthorized users. The data which came from another network or source is gathered in a server of cloud and is monitored by the users directly. Only trusted users can use the protective data and others, includes Cloud Service Providers, will not get any data of the information. Moreover, data users assume to make use of cloud data methods fully, for example data search, and data sharing, data computation overhead without disclosing of the information material to CSPs or any other third party.

Data Access Controllability: The access controllability defines that a data user can access and execute the particular limits to their data present in a cloud. The authorization of the Legal users by the user to use the data, so that others cannot use this without permissions. Moreover, it is necessary to force the fine-grained use of control to the data which can be outsourced, i.e., different owners may be given different facilities for access with respect to various data material. The checking to access the data should be monitored only by the user in the environment of cloud.

Data Integrity: Data integrity asks for maintaining the accuracy and completeness of data while sending it to the receiver. A data user always waits for which their data in a cloud can be maintained properly and with reliable method. This means for which the data would not be modified, deliberately deleted, changed, or maliciously removed. If any unnecessary methods modify or remove the data, the user may be required to find the limits of the data. Moreover, when a part of the data is changed or deleted, it can still be recovered by the data users[30].

Cloud security architecture is efficient only if the proper implementations are done. Effective cloud security architecture should find the issues which will came with security management. The security management finds these issues with various controls of security. These controls are taken into account to make it safe and any weaknesses present in the system and reduce the risk of an attack. While there are various types of controls in cloud security architecture, they can mostly be found in one of the following types:

Deterrent controls: These controls mostly, are used to reduce the attacks on a cloud. For example a warning sign on a property, deterrent controls mostly reduce the risk level by potentially informing the attackers that there will be adverse results for them if they proceed and some make them as a subset of prevention controls.

Preventive controls: Preventive controls make the system strong against some incidents, mostly by reducing if not really eliminating threats. The user's strong authentication in cloud, for example, makes it least likely that the unauthorized users can use the cloud systems, and more likely that cloud users are positively searched.

Detective controls: Detective controls are taken into account to find and control it appropriately to some incidents which occurs. In an event of an attack, a detective control will gives a sign of the preventative or corrective controls to find the issue. The network security monitoring, including the detection of the intrusion and there

are some prevention arrangements, which are mostly employed to detect attacks on cloud and the infrastructure for supporting communications.

Corrective controls: Corrective controls decrease the limitations of an incident, typically by limiting the damage. They come into account during or after an incident. Restoring system backups in order to reconstruct a vulnerable system is an instance of a corrective control.

1.3 Attribute Based Encryption

Attributed based encryption (ABE), gives a methodology by which we can be sure that, if the storage is limited, the loss of data will only be less and minimized to extent. It efficiently binds the control of access policy for the information and the owners or other clients in case of having a server which have generally access of files. ABE can be characterized into two parts depends that whether the attributes are applicable in the cipher-text or whether the access-structure is applying in the cipher-text [19]. The first was the Key-policy based ABE (KP-ABE) that is the initial form of attribute based encryption which was developed. In KP-ABE they modify the attributes along with the data and provide the access structure to every user as a bit of their secret key. But attribute based encryption is more suitable in the present world if the access-structure which be used in the cipher-text and the users must have their attributes present in their secret keys. The second form of ABE is called as cipher-text-policy based (CP-ABE)[24]. Both these present schemes were heavily depends on the sharing of secret scheme. This may be largely due to the fact that CP-ABE presents a simple and more suitable way to know the attributes based encryption.

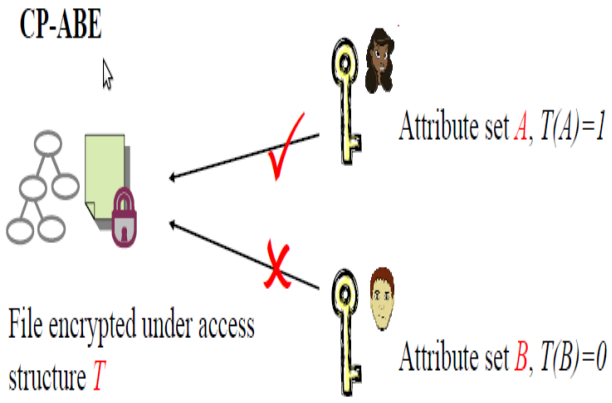

Figure 1.3: Use of correct set of attributes for decryption[32]

1.4 Homomorphic Encryption

Homomorphic encryption is a type of encryption which asks for the computation overhead to be taken out on ciphertext, hence providing an cipher form which, when converted into plain text, corrects the outcome of methods applied on the decipher text.

This is necessary, sometimes, characteristics in today's transferring method having different compound. Homomorphic encryption will asks for the collaboration of the data joined with various applications without providing the information to any of the applications. For instance, different methods of various services from various companies can check the currency exchange tax, the rate and the shifting, on a transfer without giving it to any of the unauthorized user for decrypted data to any of those applications. Homomorphic encryption methodology is presented by design. This makes it to their use in cloud computing methodolgy for providing the confidentiality of processed data[20]. The construction begins from a somehow homomorphic encryption method, which is minimized to make it to less degree parameters for the cipher data. It is minimal as every encrypted data is corrupt in little extent, and this booming become more with addition and multiplications of ciphertext, and therefore the corruption of the data makes it unnecessary. The construction begins with somehow homomorphic encryption method, which is minimal to evolving to less degree values for the cipher data. It is minimal because every encryption is corrupt in various cases, and this corruption increases with adds and multiplies of encrypted data, unless and hence the corruption will have the encrypted data into plain text[25]. This, then shows, how to modify it with minimal effect and this method to make it bootstrappable, i.e., able to defines its own decryption method and then only one operation is used in the end.

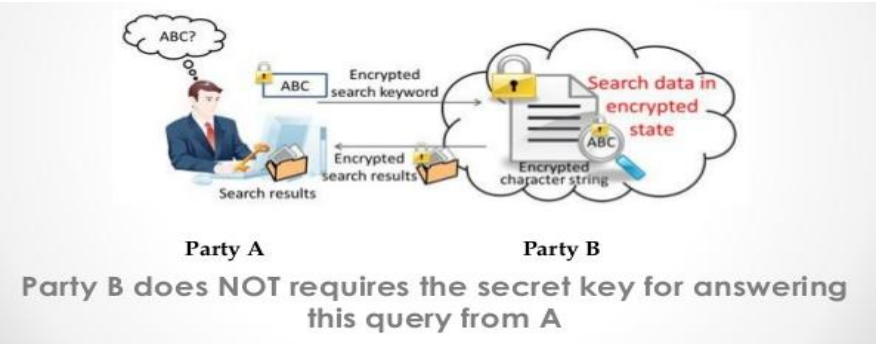

Figure 1.4: Homomorphic Encryption[33]

1.5 Diffie–Hellman Key Exchange

Diffie–Hellman is a exchange of key which is a suitable method of safely exchange the encrypted keys on a public path and is the major and initial public key technique as initially idealized by Ralph Merkle and the name given after Whitfield Diffie and Martin Hellman. Diffie Hellman is the major and advanced feasible instance of public exchange of key executed in the area of encryption[26].

In previous years, safe cryptographic transmission between the two users in which it is necessary that the first interchange keys through using some safe physical path, for example paper key provides transferred by the authorized path. The Diffie–Hellman which is a exchange of key is a method which permit two parties which has no previous information of all the users to mutually develop a transferring key which is a secure key on an unsafe path[27]. This key which may be used to cipher parallel transmissions by having a symmetric key crypto-system.Diffie Hellman can be used to safeguard the different Internet services. Moreover, the research shown in October 2015 provides the framework for the use in various Diffie Hellman Internet services at the time are somehow weak to prevent high risk data with the hackers and attackers, for example the security policies of large organizations.

The project was initially published by Whitfield Diffie and Martin Hellman in 1976, but in 1997 it was disclosed that James H. Ellis, Malcolm J. Williamson and Clifford Cocks of GCHQ, the British indicates intelligence agency, had shown previously that how public-key encryption could be attained. Moreover, the agreement for Diffie Hellman key itself is a non-authorized key-agreement service, it gives the method for many different authenticated services, hence, is used to give basis for forward security in Transport Layer Security's ephemeral nodes (referred to as EDH or DHE depending on the cipher suite).

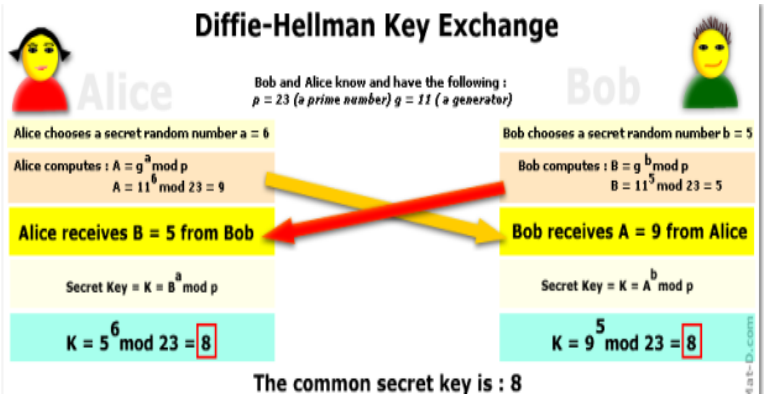

Figure 1.5: Diffie–Hellman key exchange[34]

CHAPTER 2

REVIEW OF LITERATURE

SU Mang, LI Fenghua, SHI Guozhen, GENG Kui, XIONG Jinbo (2016) [1]: In this paper, the author has discussed about the attribute based encryption(ABE) in which a collection of attributes are used for the encryption. Also cipher text policy is used in which data is accessed and controlled in cloud storage. The Proxy re-encryption technology is basically advised in order to handle the large calculations. Further, it also provides support for implementation of ABE and Identity based encryption (IBE). The proxy re-encryption divides the plain text into different parts and uses the different private keys for different parts for plain text. The Decisional Bilinear Diffie-Hellman algorithm is used. In this, a parameter is taken by using a generator say g and a key is generated. After that, the encryption is done. This process of generation of key and re-encryption is done in order to increase the security. The Proxy re-encryption algorithm reduces the computational overhead and key management.

Lifeng Li, Xiaowan Chen, Hai Jiang (2016) [2]: In this paper, the author has discussed the key management and encryption and decryption process. The cipher text policy to be analyzed for the attribute encryption is done to identify its performance and multithreading technique is used for encryption and decryption. To increase the speed of the large processes such as generation of keys, encrypting and decrypting of the data, the parallelization of cipher text policy is used to have better performance. CP-ABE takes an algorithm called AES-CTR to reduce the threats and weaknesses in AES-CBC (Cipher Block Chaining). In AES-CTR, all data sets are alone for full simultaneously and direct data permission is supported. Results for performance are achieved by the flexibility of the algorithm used. Finally, AES-CTR uses processing to speed up the encrypting and decrypting further.

HUANG Qinlong, MA Zhaofeng, YANG Yixian (2015) [3]: In this paper, the author discussed that the work is related to sharing of data to keep in mind the safety and privacy of the information. The data that is in encrypted form and has to share on the network requires the management of key. Hence, the keys for decryption should be given to the authorized user which can be less scalable and flexible. The attribute based encryption scheme will be considered as a good method for having better scalability and flexibility. In this paper, the homomorphic encryption is used in which

mathematical operations are used to solve the key escrow problem [3]. Homomorphic operation is done on the cipher text to make it more difficult for the third party and hence, cannot access the data to be transferred on the network. The homomorphic operation is donated by which is used as a symbol during encryption.

For encryption, a plain text is taken and a public key after a generation of a public key which is denoted by C = Enc (PK, M) where C is the cipher text and in the same way decryption is done ie., M = Dec(SK,C)where SK is considered as a secret key. After that homomorphic encryption is done on the cipher text by taking two cipher texts ie., C1 and C2. By applying homomorphic algorithm the cipher text will be as:

$$C = C1 \oplus C2. \quad \text{....(i)}$$

By using the homomorphic algorithm in ABE, the security can be checked whether it can be done to have security and privacy or not. The data is secured as the user who has the correct set of attributes can only decrypt the data. If the user has not right or correct attributes cannot get the information as the user is considered as an un-authorized person. If the user stores the old cipher text and use a set of attributes then also he cannot decrypt the data.

Xianping Mao, Junzuo Lai, Qixiang Mei, Kefei Chen, Jian Weng (2015) [4]: ABE gives a methodology of hard permission control over the encrypted form of data. Moreover in various ABE machine, the unit of the ciphertext and the decrypting up above, which that grows along with the hardness of an access policy, and will become unfavorable blockage in the process which is implemented on resource-based systems. Way out for decrypting of ABE cipher-texts to the any another user is a significant way to outcome the issues. As the user is mostly agreed to be unauthorized, the necessity of the security of ABE along with way out the decryption should be involved safely and justified. Although, any opponent involving the party could read and nothing is learned about the cipher text, and the accuracy of way to out plain text is meant to be checked effectively. The paper suggests general establishments of CPA security and also RCCA-safe ABE machines with secure decrypting which is the way out from CPA-secure ABE with way out for plain text. The paper also initializes the CPA-secure formation in the basic architecture and then provides a working of this instance. The research result provides the, comparison with the initial techniques; the CPA-secure establishment has many dense encrypted message and minimum costs. However, the algorithm includes among RCCA-secure

establishment may be applicable in general establishment of CCA-security of ABE, that can believed to be a single interest.

A. Abbas and S. U. Khan (2014) [5]: Cloud computing has appeared as a computing structure which is new in a sector of healthcare and various domains of business. A large number of health organizations have initiated the transferring of the information related to the electronic health in a cloud server or environment. Providing the facilities of cloud in a sector of health only make possible the transfer of records of electronic medical in the hospitals and the clinics, but makes the cloud behaving as a storage center for the record of medical. Moreover, transferring in the environment of cloud makes the organizations of healthcare of the uniteresting methods of management of infrastructure and limits the development methods and costs of maintenance. Moreover, the health data of patient is stored in the another party servers also provides many threats to the data security. As because of likely closure of entails files of medical stored and shifted in a cloud, the security of the patients concerns should importantly be examined when developing the security and safety methodologies. The various techniques have been taken into account to secure the security of the data of health records in a cloud environment. The survey formulates to encircle the state-of-the-art privacy preserve techniques provided in the clouds e-Health. However, the security preserving techniques are differentiated into various approaches and non-cryptographic techniques and classification of the techniques is also provided. Moreover, the strengths and limitations of the present techniques are noted and various open issues has been highlighted.

Junbeom Hur (2013) [6]: In this paper, the author discusses about the attribute authority which can have the attribute keys to decrypt the data. This is because there is some key escrow problem. So, the author decides to have multiple attribute authorities. The different authorities have different work ie., they have to generate only one part of the key. With this the authority cannot able to detect the exact key as they do not have the whole key to decrypt the information. The user key issuing protocol includes the generation of key center and the data-storage center. In the protocol, a user will communicate with the users before having a collection of keys.

The algorithm which is proposed by the author increases the privacy of the data and security in the data transferring system for any person for the system. There is one problem as the user has to communicate with all the authorities which can increase the

computation overhead. It increases the communication cost as the user has to contact with all the authorities.

Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, Wenjing Lou (2013) [7]: Personal health records is an efficient model for health information patient-centric transfer, that is mostly to be outsourced to be preserved at another party, for example, cloud providers. Moreover, there had been large security concerns for the information of personal health which can be seen to those extra user servers and to insecure parties. To make the patients assured, control on access to their PHRs, it is an efficient method to make a complexity of the PHRs before to be outsourced. Yet, some issues which are risks of exposure of privacy, scalability in management of key, flexible provisions, and user revocation efficiency, has remained the most important risks towards getting fine-grained, cryptographically efficient data access control. In this paper, there is a propose of a great framework for patient-centric and a group of methods for access of data control to PHRs secured in half trusted servers. To get fine-grained and also scalable data access control for PHRs, there is a hold of attribute based encryption (ABE) method to cipher PHR document of every patient. Vary from prior data in outsource of data security, the paper focuses on the various data users practical, and distribute the owners in the system of PHR into various safe paths that generally limits the complexity of management of key for the users and the owners. A large number of patient's security is important side by side by providing multi-authority of ABE. The algorithm also provides dynamic changes for the policies for access and files parameters, handles effective on-demand parameter revocation and access for break-glass in emergency scenarios. Various logical and analytical outcomes are given which shows the security, efficiency and scalability, of the proposed method.

Junbeom Hur(2013) [8]: Smart grid provides perfect exchange and distributed networks for transferring of electricity. It keeps in mind to improvise the system of electric reliability, efficiency and security, with two-way exchange sharing of the usage of data and the dynamic requirement of operations for the system of electric, and planning, maintenance. Hence, the smart grid system uses powerful power grid requirements to show efficient grid reliability and scalability. The way to achieve this is safely transferring of the calculations in grid values on large area networks. Moreover, the transferring follows techniques that depends on generator of data and the selection of consumer and have time sensitivity of data. In intelligent grid, the data

and policies for transferring the data can be at risk because it contains directly high risk information, and expose data about repressed data shielded by the techniques, and about a user and recipients of data. In this study, there is a proposal of an attribute-based scheme transferring method in intelligent grid. The data and the usage of techniques are unclear in in various points of grid operators while the data transfer method. Hence, the data security and method security are stored in the new technique. The technique for access may be provided with a random access method. Hence, the expose of the technique is increased. The safety is also improvised so that the illegal generation of key grid or the center manage machines which stores the data may not be decrypted the data to be transferred. The time for the computation users also limits by reducing mostly the complex decryption mechanisms to the stronger grid systems for the management.

Junbeom Hur (2013) [9]: The most useable and scattering of the information transferring programs in various connected systems for example, social network and cloud computing, there is an rapid increase of concerns and demands for connected data safety. One major challenging issues in data transmitting machine is the implementation of permission techniques and the policies updates support. Ciphertext technique for ABE is having a effective technique to solve this issue. It makes the data users to explain their own ways of permission for user attributes and makes the ways on the information to be shared. Moreover, the benefit generated by a large limitation that is called problem for key escrow. The center for key generation decryption could have many message addressing to various worker by originating the private keys. That's not good for information sharing examples where the data users likely to have their personal information only available for authorized users. Moreover, providing CP-ABE for the information transferring system gives one more challenge with respect to revocation of worker as the authorized ways are introduced only for the everyone. Hence, this study says, there is a need of a novel CP-ABE technique for a information transferring method by exposing the features of the outline of system. The suggested method characterize the chased goals which is the main reason for escrow problem which can be resolved by protocol of escrow-free key issue, which can be established using safe two-way communication in-between the data-storing center and key generation center. The revocation for fine-grained worker for each parameters can be completed by proxy encrypting that takes advantage of the selected parameter group distribution of key on the start of ABE.

The security analyses and the performance provides that the suggested method is effective to safely handle the information divided in the information transferring system.

Kan Yang, Xiaohua Jia, Kui Ren, Bo Zhang (2013) [10]: Information permission control is an enough to make suer the information safety in the cloud. Moreover, due to way out of data and unauthorized cloud servers, the permission control for data converted into a large problem in saving devices of cloud. The current permission control techniques are not enough to saving devices of cloud, because they may produce various encrypted form of information which are the copies of similar data and require a authorized cloud server. CP-ABE is a enough method for accessing of control of encrypted message. An authorized authorities required which can manages all the distributes keys and the attributes in the machine. In systems of cloud saving, there are various people that co-exist and every person is required to provide parameter separately. Moreover, the existing CP-ABE technique can't be applicable to control of information for accessing for multiple authorities systems for cloud storage, due to the ineffective of revocation and decryption. In this paper, there is a proposal of DAC-MACS (Data Access Control for Multi-Authority Cloud Storage), an efficient and safe data access control technique with effective revocation and decryption. Importantly, there is a construct of a proposed multi-authority CP-ABE technique with effective plain text and hence also define an effective method for attributes revocation which can get the backward security and forward security. The precise monitoring and the simulation outcomes gives that the DAC-MACS is greatly effective and provably secure in the safe model.

Xun Yi, Mohammed Golam Kaosar, Russell Paulet, and Elisa Bertino (2013) [11]: PIR provides a worker to get the ith number of an n-bit storage without exposing to the server for the database, the result of i. In this, there is a presentation of a PIR protocol which also has transferring problem of Oð log nÞ bits, in which ð is the unit of the ciphertext. Moreover, there is a expansion of the PIR for a PBR protocol, a normal and more executable expansion of PIR in that the worker gets a set of bits, inspite of getting one bit. The protocols is formed on the state-of-art for FHE methodologies and provides security for the users if FHE method is definitely secure. The entire transferring difficulty of the PBR is Oð log m þ n=mÞ bits, where m = number of blocks. The all over computation difficulty of the PBR is Oðm log mÞ modular multiple times plus Oðn=2Þ modular adds ons. In terms of entire protocol

execution time, the PBR protocol is higher effective than the existing PBR protocols which definitely required to execute Oðn=2Þ modular multiplications when the set size in the database is large and a high-speed network is available.

Zhiguo Wan, Jun'e Liu, and Robert H. Deng (2012) [12]: Cloud computing has come out as major and the most powerful method in the IT industry in some years. As this new computing technique require users to make their important data entrusted to the cloud providers, there has been increased safety and security factors for data to be outsourced. Various schemes providing and uses attribute-based encryption has been implemented for having control of data to be outsourced in cloud computing. Moreover, many of it suffers from ineffeciency in introducing difficult access control policies. Therefore, to have flexible, fine-grained and scalable, access control for data to be outsourced in cloud computing. So, in this paper, there is a hierarchy of attribute-set based encryption (HASBE) by expanding ciphertext-policy attribute-set-based encryption (ASBE) along with a hierarchichy of structure for users. The new scheme not only provides scalability as of its hierarchy of structure, but also provides fine-grained permission of control and flexibility in support of various attributes of ASBE. Moreover, HASBE provides various papers for different values for accessing last method to work with revocation of user more effectively than already existing system. The paper defines the safety of HASBE which depends on safety of the ciphertext-policy attribute-based encryption (CP-ABE) method by Bethencourt et al. and monitors its computational complexity and performance. It is implemented and shows that it has an effective and flexiblity in handling with permission of control for data to be outsourced in cloud computing with complex experiments.

J. Hur (2011) [13]: In this paper, the author discusses about the issues for the data to be transferred on the network, the policies which are authorized are used and the policy updates are also taken into account for further use. Cipher-text-technique attribute-based encryption has a good cryptographic answer to these problems for using the access control methods explained by a data user on the information which is coming from the sender. However, there is an issue of using the ABE in an outline defines which includes many issues with respect to the parameter and revocation of user. In this the author proposes an permission control method which is having ciphertext-policy ABE in order to change the permission control policies with enough parameter and user revocation capability. The fine-grained permissive control can be generated by dual encryption method in which attribute based encryption is used and

the set of keys are taken in order to encrypt the data. There are some examples of how to use the suggested method to safely manage the data which can be external or internal. The studied results show that the suggested method is enough and safe in the data outsourcing systems. The dual cipher protocol destructs the joined characteristics of the cipher-text policy attribute-based encryption and group key management algorithm. The new technique allows the user to explain the control of access policy and make it on the data which can be internal and external.

Junbeom Hur and Dong Kun Noh (2011) [14]: There are various problems in outsourced data scenario which are the establishment of permissive techniques and the policy updates support. CP-ABE is a effective cryptographic answer to some problems for making permission control techniques explained by an owner on information to be outsourced. Moreover, the issue for using the ABE in an outline to be outsourced provides various issue with regard to the user revocation and attribute. In this paper, an permission control method is using CP-ABE to make the permission control policies with effective user revocation features and attributes. The fine-grained permission control can be aimed by dual encryption method which takes benefit of the ABE and have a group key distribution in every attribute group. There is a demonstration of how to have the proposed scheme to safely manage the data to be outsourced. The analysis results provides that the proposed method is effective and secure in the outsourced data systems.

Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou(2010) [15]: Cloud computing has an effecient computing method in which the services of the architecture to be computed are given as methods on the Internet. However, this computing also provides forth various new challenges for the security of data and control of access when users sends the high risk data for transferring on cloud servers, that are not in the same authorized domain as of data owners. The sensitive user keeps the data confidential against unauthorized servers, available solutions normally applicable with cryptographic methods by sharing data decryption keys only to trusted users. Hence, by doing so, these solutions continuously introduce a great overhead for computation for the data owner for distribution of keys and management of data when fine-grained data access control is required, and hence, good scaling is not done. The problem of continuously getting scalability, fine-grained-ness, and data confidentiality of control of access and hence still remains mystery. The paper keep into account this major issue is opened, in one hand, providing and expanding policies of access which

is depends on attributes of the data, and, in the other hand, allows the owner of the data to implement various computation job involved in fine-grained access of data control to unauthorized servers of cloud without exposing the various data contents. By achieving this aim by expanding and uniquely joining the methods of proxy re-encryption, attribute-based encryption (ABE), and lazy re-encryption. The new technique also has effective properties for privilege for user access having secret key accountability and confidentiality of user. The expanding analysis provides that the proposed system is greatly effective and efficiently secure in the existing security technique.

John Bethencourt, Amit Sahay Brent Waters(2007) [16]: In various different systems, a person can access data if a person is having a various set of attributes or credentials. Now a days, the only technique for expanding such techniques is to have a authorized server to make the data to be stored and starts the access control. Moreover, if any server having the data is understandable, then the security of the data will be understandable. In the paper, there is a machine for having a difficult access control for the cipher data that is called Ciphertext-Policy Attribute-Based Encryption. As using these new techniques, the cipher data can be having a security even if the server of storage is unauthorized. Hence, the proposed techniques are safe against various attacks. The prior Attribute-Based Encryption methods were using parameters to define the encrypted data and establish techniques into user's keys. As in proposed system, the parameters have to define the information of users, and a third party encrypting data define a method for those who can change into plain text. Hence, the proposed methods are explaining closer to old control of access technique for example Role-Based Access Control (RBAC). Moreover, there is an establishment of the new system and provides performance measurements.

CHAPTER 3
PRESENT WORK

3.1 Problem Formulation

The modified homomorphic encryption scheme provides the programs to be constructed for any required characteristics, which can be rushed on encrypted data to provide an encryption of the data. Since, such a functionality need which cannot be decrypting the data, it can be rushed by any unauthorized party without providing the data and its internal state. The presence of the effective and modified homomorphic algorithm would have large practical impact for the private computations to be outsourced in the cloud computing. This algorithm can be used in Attribute based encryption includes homomorphic encryption includes additive and multiplicative calculations along with Diffie hellman key exchange method. The prime numbers are used as a prime number has no factor due to which the decryption of the data is difficult by the attackers. This makes the encryption more difficult to understand and less space is used as the key generation is small in size. Also the execution time is less as compare to the existing work. So, this algorithm can be used in attribute based encryption, due to which the unauthorized users or any other third party is unable to decrypt the data.

3.2 Objectives of the Study

The main objectives of the modified homomorphic algorithm for Attribute based encryption is as follows:

- To make the data encrypted which is difficult to understand by using attribute based encryption
- To reduce the un-authorizations by using the diffie hellman key exchange algorithm
- To reduce the space utilizations by using the small bits of keys in the algorithm
- To reduce the time consumption in the algorithm
- To use the prime numbers as the prime numbers have no factors which is difficult to decrypt.

3.3 Research Methodology

The study is generally presented on to generate model for modified homomorphism disk encryption technique. The present technique will give suitable key management services and key storage. This can encompass the reliability and safety of the existing homomorphism encryption technique. In the new model, safe path development algorithm can be used for the management of key and sharing of key. The safe path development techniques are Diffie- Helman and RSA. The Diffie- Helman technique is very safe and suitable algorithm. In this Diffie-Hellman technique if two users, Master and Slave wants to transfer the data. Before the start of the sharing of data, safe path is developed. Both the users choose their own arbitrary number. Based on the selected arbitrary numbers, safe path and the key is generated.

Diffie Hellman key exchange algorithm is embedded for permission process. In the cloud network, it explains the node from where the data is to send and the destination node. To develop safe path between transferring parties, every party choose a arbitrary prime factors g and n, choosen factors will become public keys for both the users. The node from where the data transfers will became master and the destination node will become slave and the master and the slave selects the private keys ‘a’ and ‘b’ simultaneously. The master checks the new number “M” from the choosen the public and the private numbers.

$M= g^a \bmod n$

The Slave checks the new number “S” from the choosen public and the private factors

$S= g^b \bmod n$

The Master user and the slave user share their processed value “M” and “S” through the middle nodes. So, When Slave gets “M” and the Master receives "S”, then both the parties will check mode inverse value.

When the master gets the value “S” from slave and process the new value “K1” from the received “S” value.

$K1=S^a \bmod n$

Slave gets the value “M” from the master user and processes the new value”K2” through the received “M”

$K2=M^b \bmod n$

After processing K1 and K2, both the users develop the safe path, by processing the new key K. If both the users who are sharing data to each other, have same K1 and K2 values, the safe path is developed between the users

K=K1+K2

The sharing of data begins between the users when safe path is developed between between the users. The transferring of data between both the parties is secured with the public keys. Both the users uses their own private keys to decrypt the sharing of data.

The following flowchart defines the work, and how the developed Diffie-Hellman develops in safety of cloud networks.

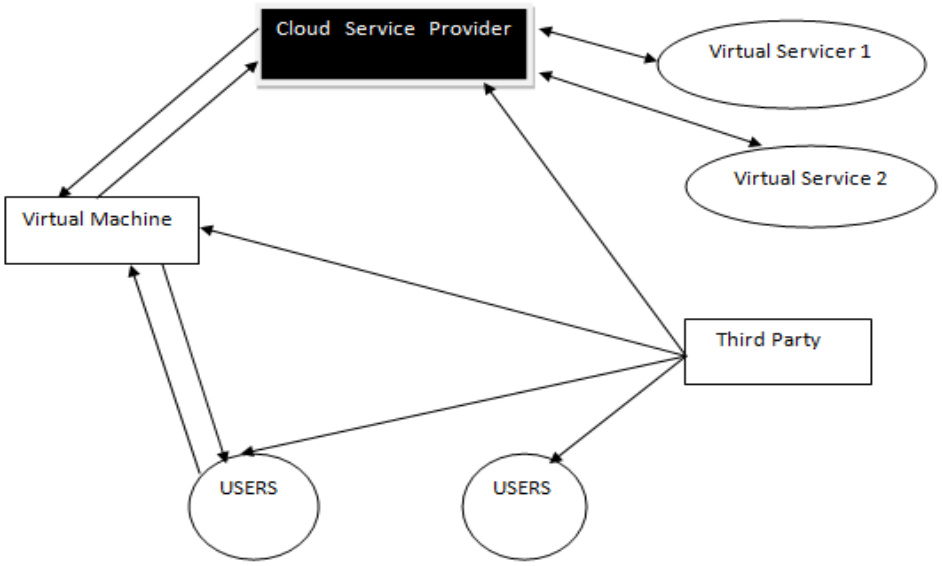

Figure3.1: Data communication diagram

In figure 3.1, a service provider cloud is shown which is related with the virtual servers bidirectionally. It is also related with the virtual machines. Hence, there are various users that are available in the network. These parties are related with the virtual machines to share the data between them. The third user is also shown in the given network. This user is joined or attached with the virtual machines, cloud service provider and the users. So, in the present work, the homomorphic encryption algorithm is used in the virtual machine. But this technique has no key transferring and the key development method. Due to this limit of this algorithm, the safety of the network is on the risk level. The chance of the attack is high in this algorithm. To solve this problem in the virtual machine, the Diffie-Hellman technique is used on the virtual machines in spite of the homomorphic encryption algorithm. In Diffie-Hellman technique, the key transferring and the key organization technique is used in it so that suitable safety is given to a network. The public and the private keys are transferred between the sender and the receiver first. Hence, after the transferring of

the keys between the users then the transferring begins between the user and the virtual machine. So, it is shown that the safe path is developed between them.

In our method, Diffie-Hellman algorithm is using for the safe channel development and for the mutual authorization. In the proposed technique, only two messages are reqired to share between the two machines and a safe path will be developed. It is safer than the present authorization process. It takes low time to authorize the parties and it expands the performance of the mobile model in the topology. Diffie Hellman key exchange algorithm gives the security against the attack. In Diffie -Hellman technique, there is no privilege for the accumulation or sharing of the PIN key. So it secures the network devices from attacks.

Algorithm:

Selected node suppose user1

1. Login
2. Key generation
   2.1 Enter prime numbers
   2.2 Enter random numbers by client and cloud service provider
   2.3Secret key generation and secure channel establishment
3. OTP (One Time Password) generation
   3.1 cloud server will set count1=0,...count5=0 for respective user at its side.
   3.2 Cloud Server will request for the OTP from user 1
   3.3 user1 enter (secret key+count) as OTP
   3.4 server match it because server knows both secret key and count of each user.
      3.4.1: count1++; // so for user 1 it will be count1=1; for remainig user their count will be still 0;
      3.3.2 if (secret_key+count(x) == secret_key+count(y))
         { Access granted;
           display message by server : print "please enter the operation";}
           else{ display message by server: print(" wrong password, your login number is count1);}
   4.4 clinet will enter the operation using HMAC digest
      4.4.1: hmac(already generated secret key || v, file1,ver1 || sha1)
         {if(ope==v)
            { server will check the file name and version;

if(file1,ver1== file1,ver1)

{print "file is valid";}

else{print file is invalid, please replace the file

}}

if(ope==I) { insert new file file2}

5. encryption/decryption

6. data operation

7. logout;

note: // 1.at client side, user will enter prime number, random number for generating secret keys, once generating secret key user will enter otp , after inserting otp, user will enter operation(Insertion) with corresponding file name(file1 or file2).//

FLOW CHART

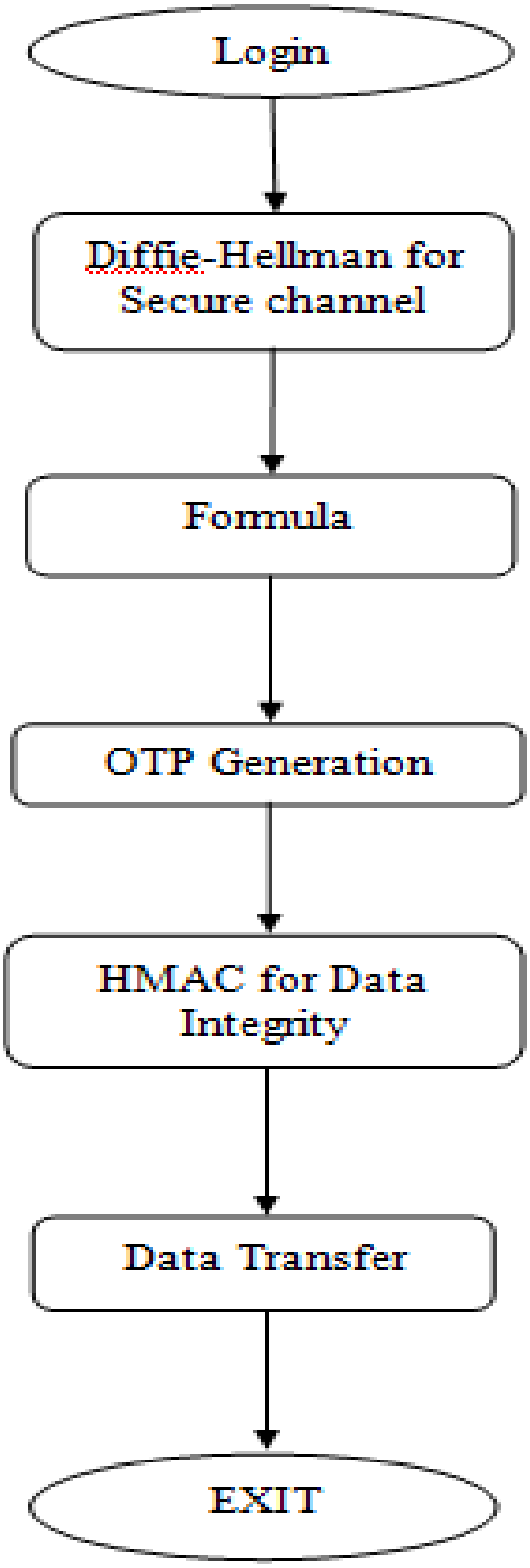

Figure 3.2:Process of the New Algorithm

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Experimental Results

1. First, the node is selected from which the data has to be transferred to cloud node in order to send to destination side.

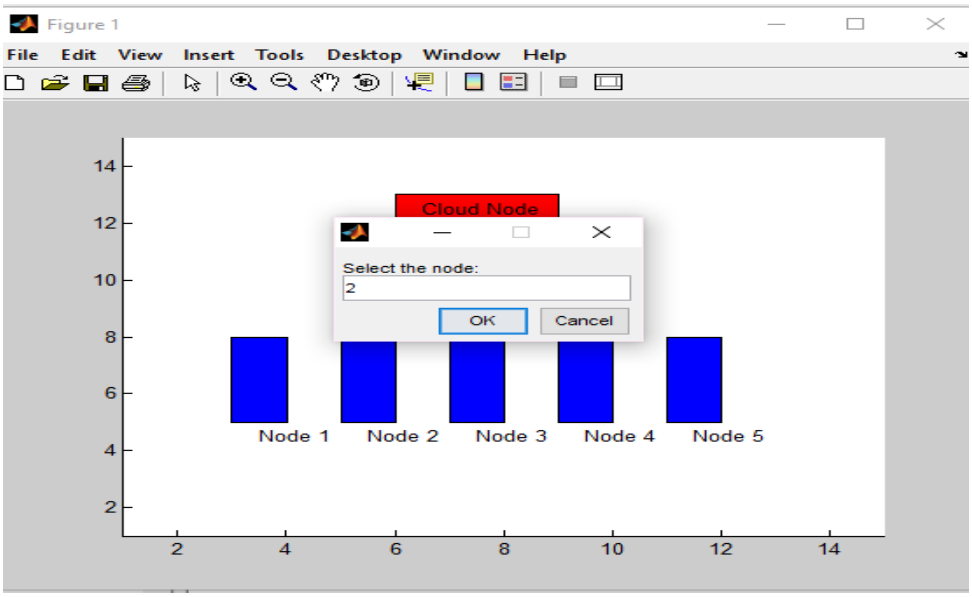

Figure 4.1: Node Selection

2. The second step is to select a key for user A in order to encrypt the data before transferring it to the cloud node.

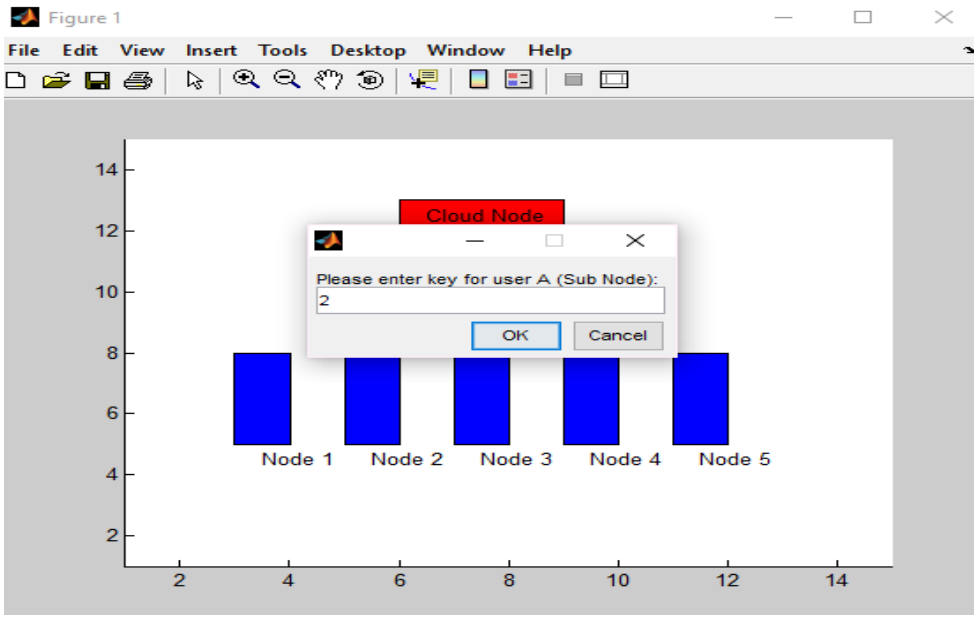

Figure 4.2: Key Selection for User A

3. The next step is to select a write operation in order to start a process of transferring of data to user B.

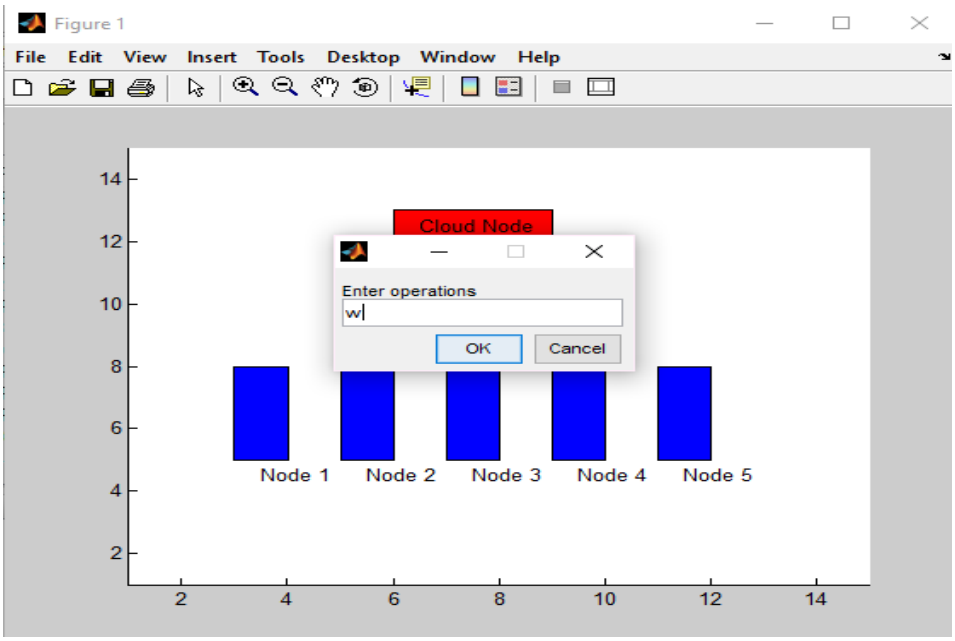

Figure 4.3: Selecting write Operation

4. The same key is also selected for user B so that it can decrypt the data after the data is received to it.

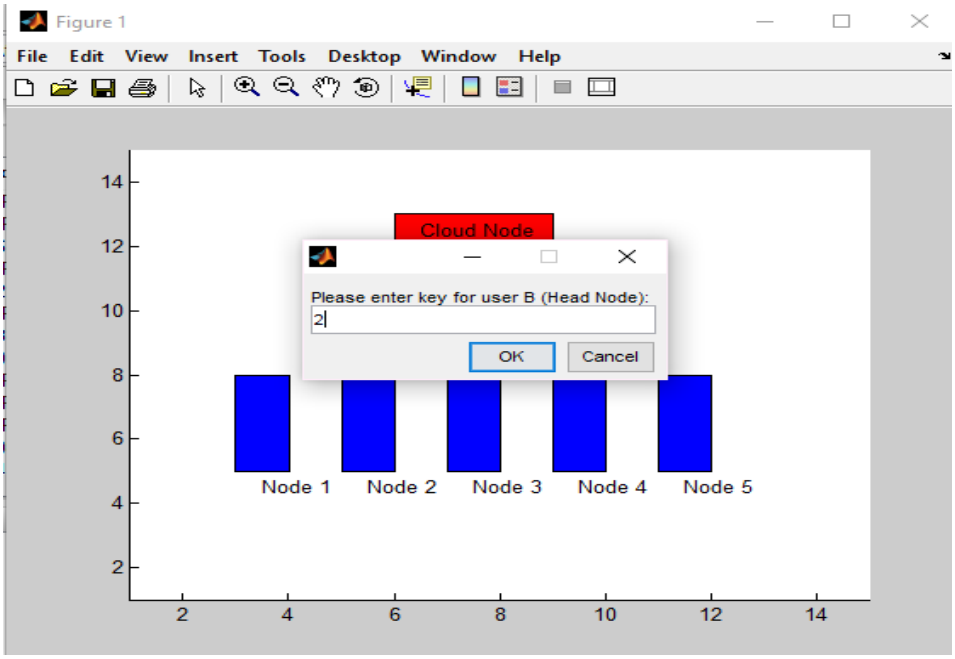

Figure 4.4: Key Selection for User B

5. The data is encrypted before transferring it to the cloud node by using simple encryption method.

6.

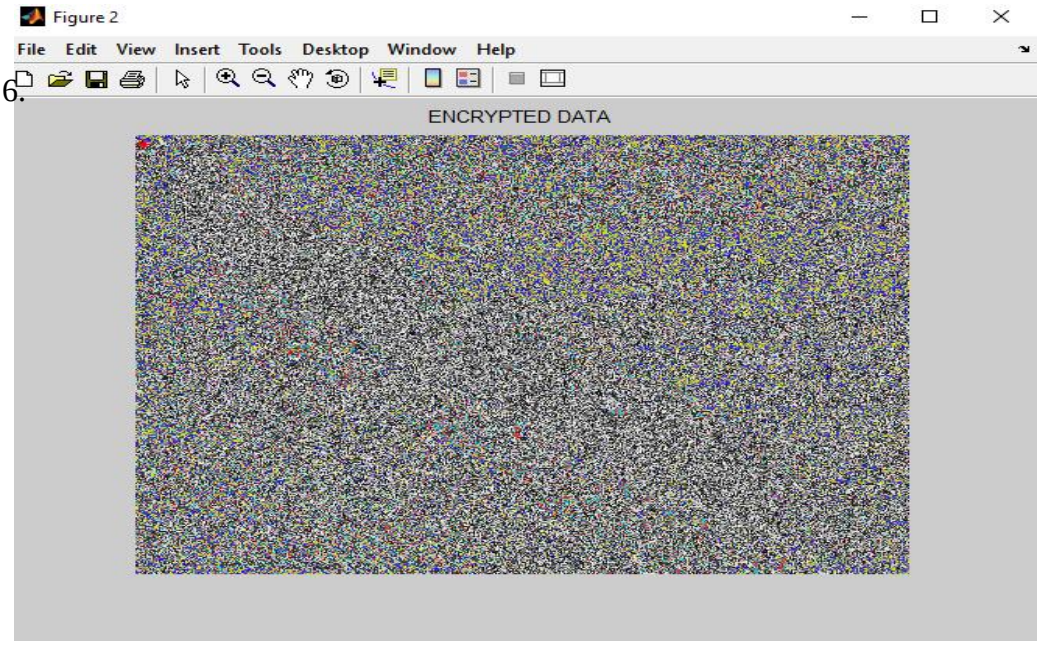

Figure 4.5: Encrypted Data

6. The node will start the sending of data to the cloud node in order to transfer it to the receiver

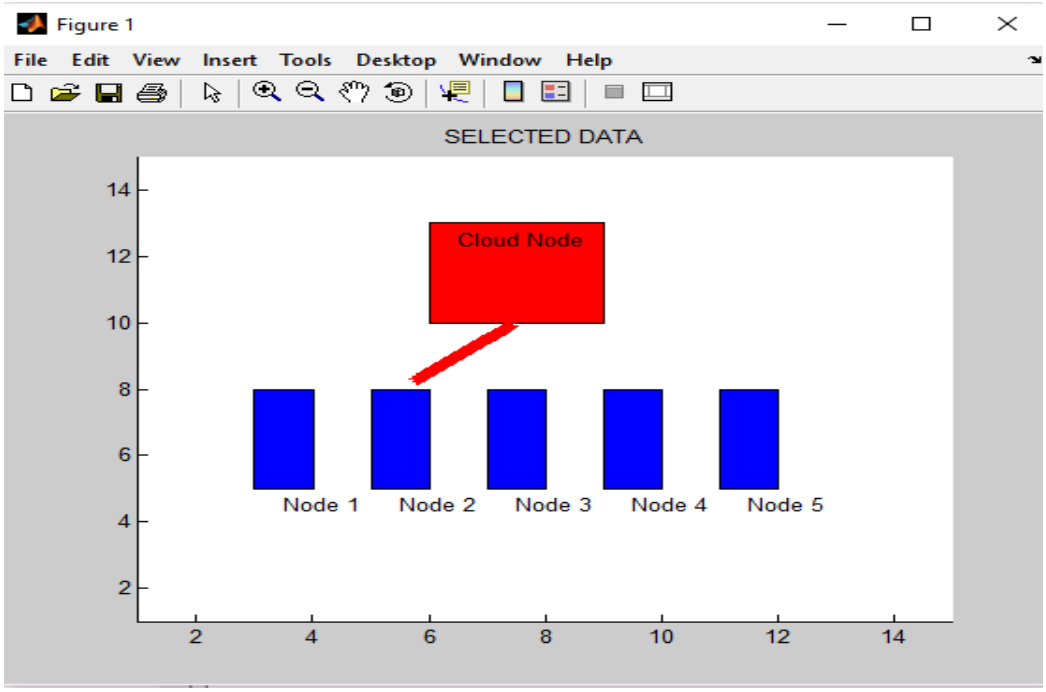

Figure 4.6: Sending Data To Cloud Node

7. The cloud node will acknowledge the node that the has been received by it to forward to the receiving node.

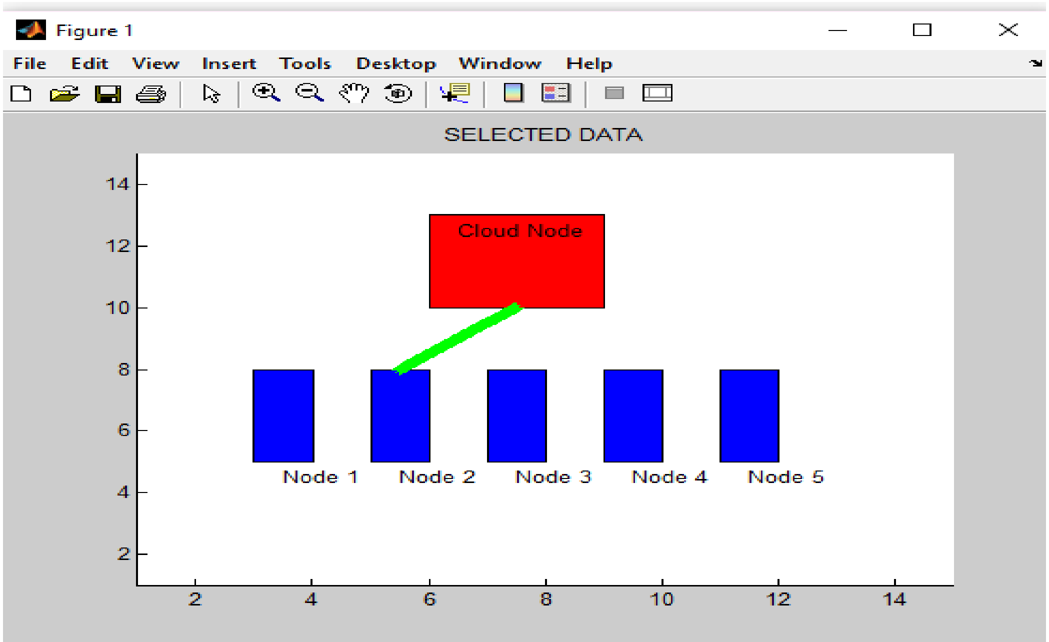

Figure 4.7:Acknowledgement of Data

8. The prime numbers are selected in order to make the encryption stronger as the prime numbers have no factors so it cannot be decrypted easily. The values for user A and B for login for the data transferring.

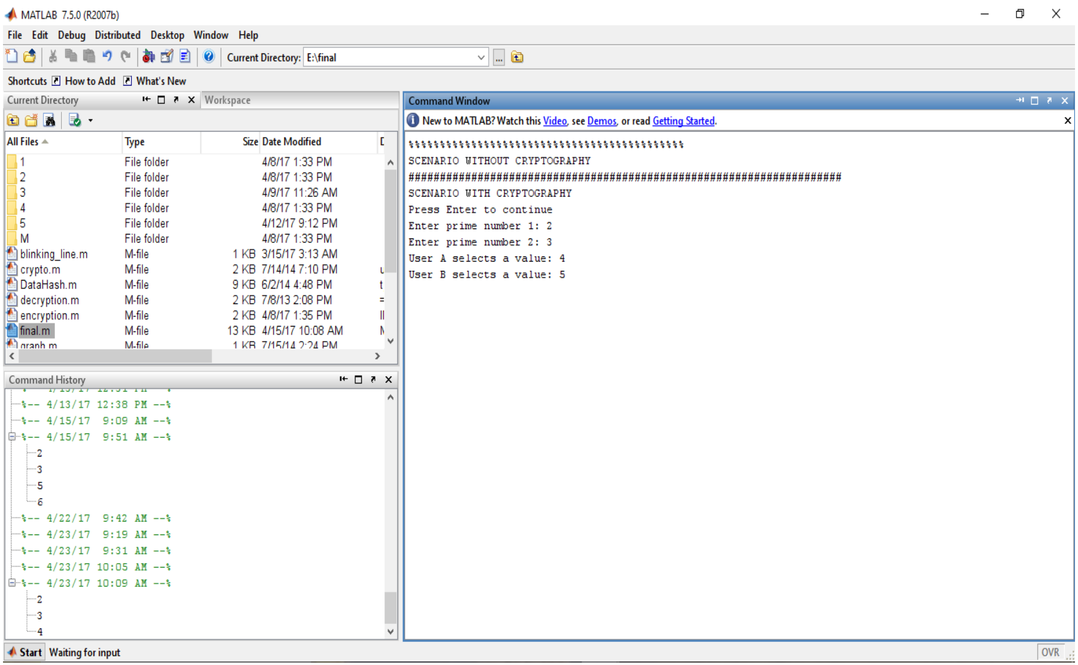

Figure 4.8: Selecting Prime Numbers

9. The secret key is generated for both user A and B and login number is entered for the login of both the users.

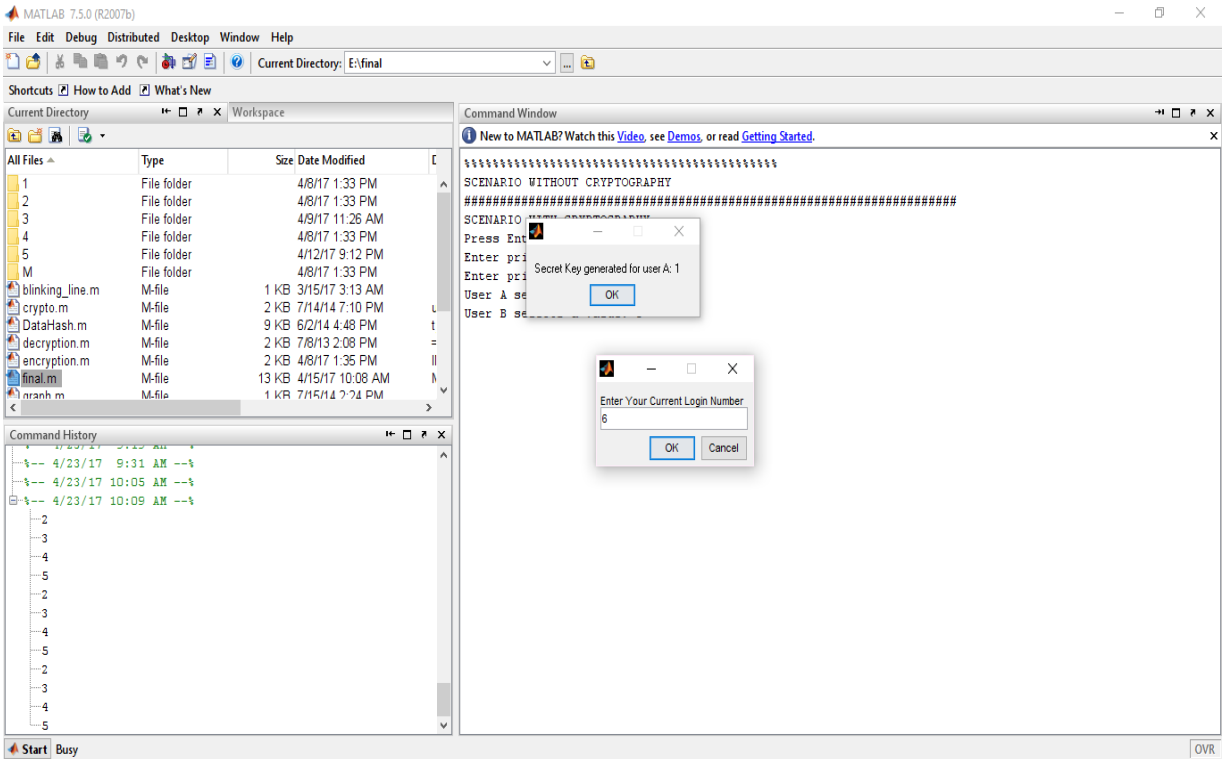

Figure 4.9:Login Number Selection

10. The one time password is calculated by adding key generation and login number.

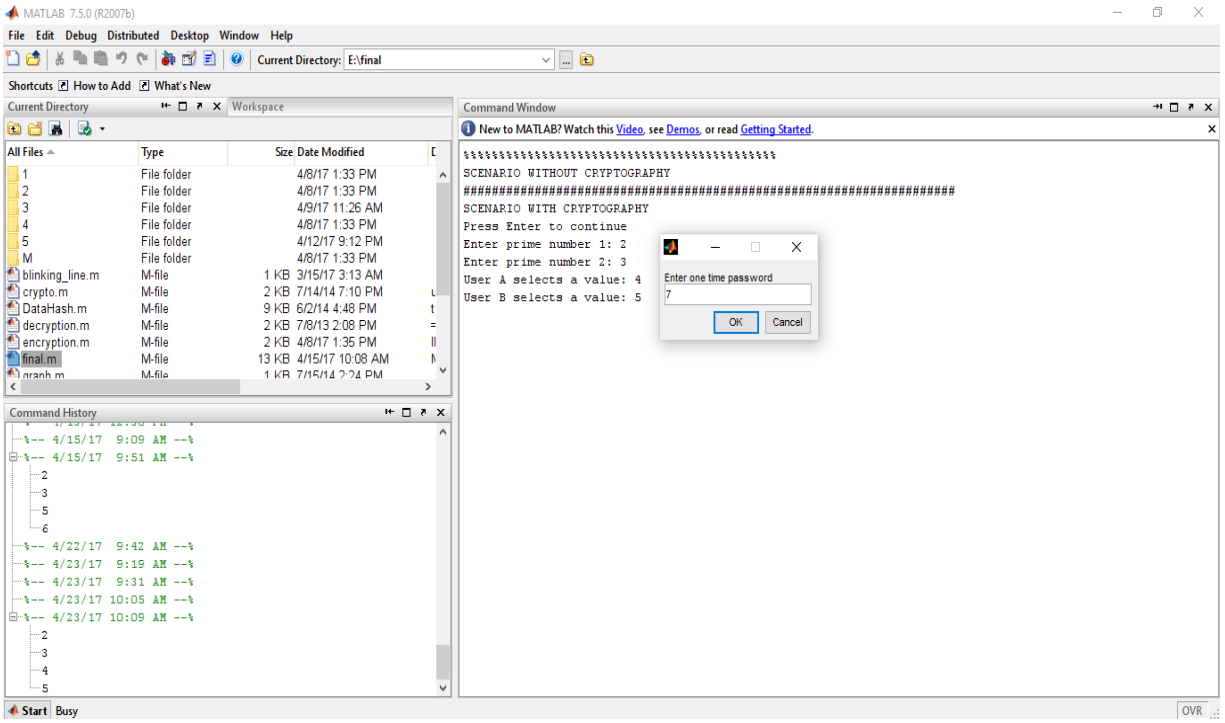

Figure 4.10: Generating OTP

11. The cloud node will send the information that the data has been received by the receiver node.

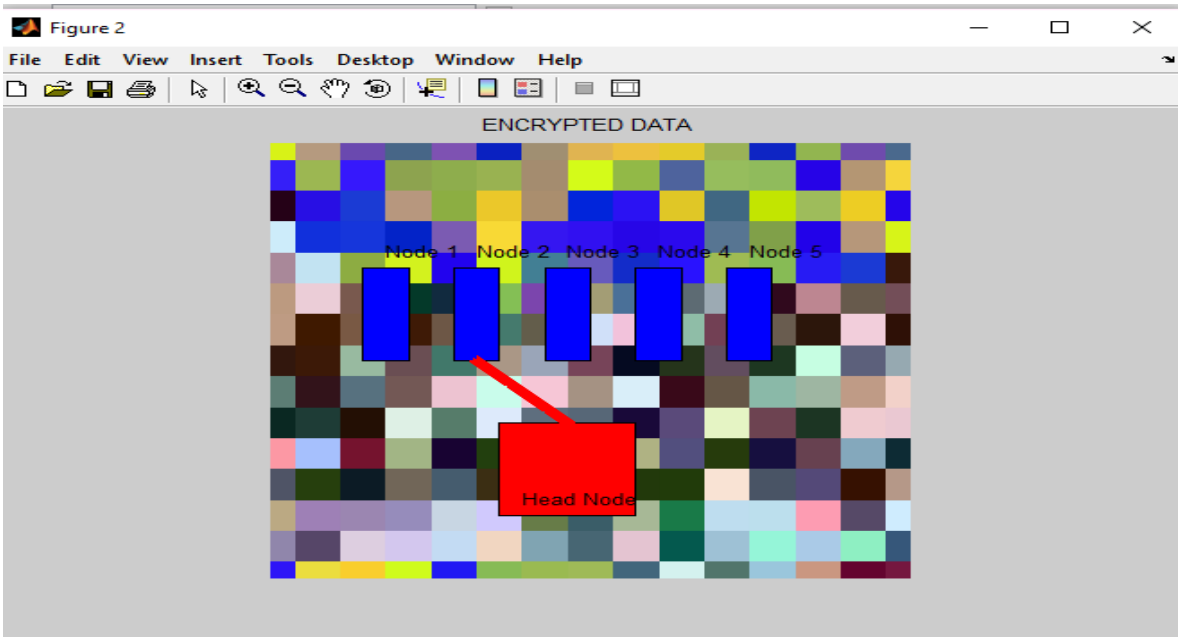

Figure 4.11: Cloud Node giving confirmation about receiving the data

12. The node will acknowledge to the cloud node that the information has been received.

Figure 4.12: Acknowledgement of receiving data

4.2 Comparison With Existing Technique

1. The key generation is small ie., the bits are small which can be stored in less space in proposed system as compare to the existing system. The small key can be selected because further prime numbers are used as public keys for encryption and no space is required for that key.

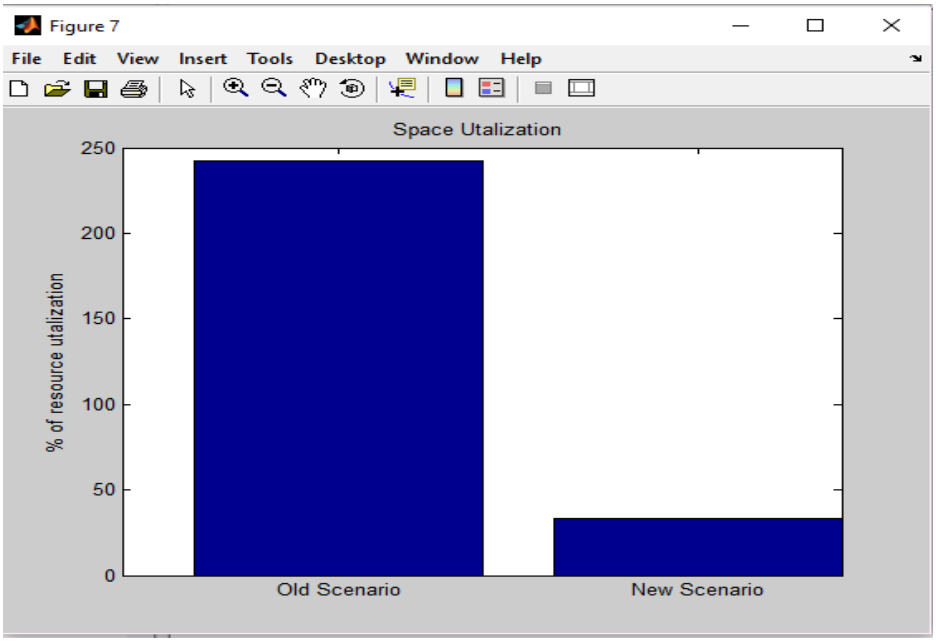

Figure 4.13: Comparison of Space utilization

2. The execution time of the proposed system is less as compare to the existing system because in existing system the resources which are used are more as compare to the proposed system.

   The method used for the execution time is as follows:

   Execution time = resources*unit(1.5)

   The execution time for the existing system is

   Execution time = 2*1.5

   = 3ms

   The execution time for the proposed system is

   Execution time = 1.8*1.5

   = 2.7ms

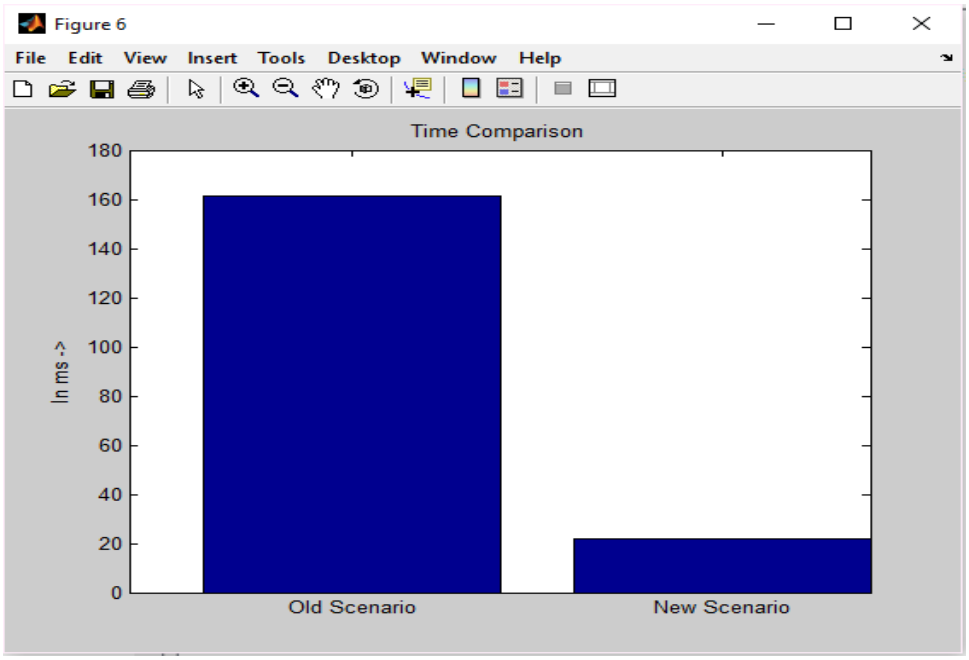

Figure 4.14: Time Comparison

Comparison of Proposed and Existing System

Parameters	Proposed Scheme	Existing Scheme
Space Utilization	More	Less
Execution Time	More	Less
Possibilities of Attacks	More	Less

Table 4.1: Comparison

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

Attribute based encryption (ABE), presents a technique through which we can make sure that if the storage is minimum, the loss of data will only be limited. It effectively makes a boundary for the policy for the access control for the data and the clients or users inspite of getting a server using access to files. It extends the scope of the computations which can be applied to process encrypted data homomorphically. Modified homomorphic includes both additive and multiplicative operations along with diffie hellman methodin which prime numbers are used. The modified homomorphic encryption is used with this to make the algorithm difficult to understand by the attackers. This is better than the homomorphic encryption as less space is used by the keys. It can be rushed by an unauthorized party without providing the data and its internal information.

5.2 Future Scope

Attribute based encryption (ABE), presents a technique through which we can make sure that if the storage is minimum, the loss of data will only be limited. The modified homomorphic encryption scheme provides the programs to be constructed for any required characteristics, which can be rushed on encrypted data to provide an encryption of the data. Since, such a functionality need which cannot be decrypting the data, it can be rushed by any unauthorized party without providing the data and its internal state. It extends the future scope of the computations which can be applied to process encrypted data homomorphically which includes additive and multiplicative calculations along with Diffie hellman key exchange method. The prime numbers are used as a prime number has no factor due to which the decryption of the data is difficult by the attackers and hence the attacks will be less as compare to the existing work. This makes the encryption more difficult to understand and less space is used as the key generation is small in size. Also the execution time is less as compare to the existing work. So, this algorithm can be used in attribute based encryption, due to which the unauthorized users or any other third party is unable to decrypt the data.

LIST OF REFERENCES

[1] SU Mang, LI Fenghua, SHI Guozhen, GENG Kui, XIONG Jinbo (July 2016), "A user-centric data Secure creation scheme in cloud computing", University of science and Tech., Nanjing, China, Vol 25, N0.4.

[2] Lifeng Li, Xiaowan Chen, Hai Jiang (June 2016), "Parallelizing cipher text policy attribute based encryption for clouds", College of Info. Science and Tech., Chin,.

[3] HUANG Qinlong, MA Zhaofeng, YANG Yixian (October 2015), "Attribute based secure data sharing with efficient revocation in cloud computing", Information security center, Beijing, China, vol 24, No. 4.

[4] Xianping Mao, Junzuo Lai, Qixiang Mei, Kefei Chen, Jian Weng (November 2015), Generic and Efficient Constructions of Attribute-Based Encryption with Verifiable Outsourced Decryption", Volume: 13, pgs 533-546.

[5] A. Abbas and S. U. Khan (2014)," A Review on the State-of-the-Art Privacy-Preserving Approaches in the e-Health Clouds", Volume: 18, Pages: 1431 – 1441.

[6] Junbeom Hur (October 2013), "Improving security and efficiency in attribute based data sharing", vol 25, No. 10.

[7] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, Wenjing Lou(2013),"Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption", *IEEE Transactions on Parallel and Distributed Systems*, Vol.24, No.1, pp.131–143.

[8] Junbeom Hur(2013), "Attribute-based secure data sharing with hidden policies in smart grid", *IEEE Transactions on Parallel and Distributed Systems*, Vol.24, No.11, pp.2171–2180.

[9] Junbeom Hur (2013), "Improving security and efficiency in attribute-based data sharing", *IEEE Transactions on Knowledge and Data Engineering*, Vol.25, No.10, pp.2271–2282.

[10] Kan Yang, Xiaohua Jia, Kui Ren, Bo Zhang (2013) "DAC-MACS: Effective data access control for multi-authority cloud storage systems", *Proceedings of IEEE INFOCOM 2013*, Turin, Italy, pp.2895–2903.

[11] Xun Yi, Mohammed Golam Kaosar, Russell Paulet, and Elisa Bertino (2013), "Single-database private information retrieval from fully homomorphic encryption", *IEEE Transactions on Knowledge and Data Engineering*, Vol.25, No.5, pp.1125–1134.

[12] Zhiguo Wan, Jun'e Liu, and Robert H. Deng (2012) A hierarchical attribute-based solution for flexible and scalable access control in cloud computing", *IEEE Transactions on Information Forensics and Security*, Vol.7, No.2, pp.743–754.

[13] Junbeom Hur and Dong Kun Noh (October 2011), "Attribute based access control with efficient revocation in data outsourcing systems", vol 22, No. 7.

[14] Junbeom Hur and Dong Kun Noh (2011), "Attribute-based access control with efficient revocation in data outsourcing systems", *IEEE Transactions on Parallel and Distributed Systems*, Vol.22, No.7, pp.1214–1221.

[15] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou(2010), "Achieving secure, scalable, and fine-grained data access control in cloud computing", *Proceedings of IEEE INFOCOM 2010*, San Diego, CA, USA, pp.1–9.

[16] John Bethencourt, Amit Sahay Brent Waters(2007), "Ciphertext-policy attribute based encryption", *Proceedings of 2007 IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, pp.321–334.

Websites:

[17] https://en.wikipedia.org/wiki/Cloud_computing

[18] https://en.wikipedia.org/wiki/Cloud_computing_security

[19] https://en.wikipedia.org/wiki/Attribute-based_encryption

[20] https://eprint.iacr.org/2015/1192.pdf

[21] http://searchcloudcomputing.techtarget.com/definition/cloud-computing

[22] http://www.globaldots.com/cloud-computing-types-of-cloud/

[23] http://searchcompliance.techtarget.com/definition/cloud-computing-security

[24] https://www.slideshare.net/prosunjit/attribute-based-encryption

[25] http://searchsecurity.techtarget.com/definition/homomorphic-encryption

[26] https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

[27] http://searchsecurity.techtarget.com/definition/Diffie-Hellman-key-exchange

[28] https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/

[29]http://erpbloggers.com/2013/07/the-five-essential-characteristics-of-cloud-computing/

[30] http://tec.gov.in/pdf/Studypaper/Paper-1-security%20and%20Privacy.pdf

[31] https://www.slideshare.net/cloudgenius/9-cloud-computingsecurity

[32] http://mohamednabeel.blogspot.in/2012/03/aattribute-based-encryption-abe-and-its.html

[33] https://www.slideshare.net/iamrandomizer/homomorphic-encryption-53238006

[34]http://stackoverflow.com/questions/28015433/is-it-possible-to-hack-diffie-hellman-by-knowing-the-prime-number-and-the-gene

ORIGINALITY REPORT

%7	%4	%5	%
SIMILARIT Y INDEX	INT ERNET SOURCES	PUBLICAT IONS	ST UDENT PAPERS

PRIMARY SOURCES

purdue.edu Int ernet Source	%1
Wan, Zhiguo, Jun'e Liu, and Robert H. Deng. "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing", IEEE Transactions on Information Forensics and Security, 2012. Publicat ion	%1
Yang, Kan, Xiaohua Jia, Kui Ren, and Bo Zhang. "DAC-MACS: Effective data access control for multi-authority cloud storage systems", 2013 Proceedings IEEE INFOCOM, 2013. Publicat ion	%1
www.science.gov Int ernet Source	<%1
www.ijcaonline.org Int ernet Source	<%1
ijarcce.com Int ernet Source	<%1

7	Wang, Jihe, Meikang Qiu, and Bing Guo. "High reliable real-time bandwidth scheduling for virtual machines with hidden Markov predicting in telehealth platform", Future Generation Computer Systems, 2015. Publicat ion	<%1
8	Lekshmi, S. Vijaya, and M. P. Revathi. "Implementing secure data access control for multi-authority cloud storage system using Ciphertext Policy-Attribute based encryption", International Conference on Information Communication and Embedded Systems (ICICES2014), 2014. Publicat ion	<%1
9	dblp.dagstuhl.de Int ernet Source	<%1
10	www.springerprofessional.de Int ernet Source	<%1
11	SpringerBriefs in Computer Science, 2014. Publicat ion	<%1
12	Wang, Yun, Dalei Zhang, and Hong Zhong. "Multi-authority based weighted attribute encryption scheme in cloud computing", 2014 10th International Conference on Natural Computation (ICNC), 2014. Publicat ion	<%1
13	ieeexplore.ieee.org Int ernet Source	<%1

14	Li, Lifeng, Xiaowan Chen, Hai Jiang, Zhongwen Li, and Kuan-Ching Li. "P-CP-ABE: Parallelizing Ciphertext-Policy Attribute-Based Encryption for clouds", 2016 17th IEEE/ACIS International Conference on Software Engineering Artificial Intelligence Networking and Parallel/Distributed Computing (SNPD), 2016. Publicat ion	<%1
15	Lecture Notes in Computer Science, 2015. Publicat ion	<%1
16	Kumari, P. Senthil, and A. R. Nadira Banu Kamal. "Optimal Integrity Policy for Encrypted Data in Secure Storage using Cloud Computing", Indian Journal of Science and Technology, 2016. Publicat ion	<%1
17	www.slideshare.net Int ernet Source	<%1
18	libres.uncg.edu Int ernet Source	<%1
19	gujs.gazi.edu.tr Int ernet Source	<%1
20	R. Mynavathi, V. Bhuvaneswari, T. Karthikeyan, C. Kavina. "K nearest neighbor classifier over secured perturbed data", 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare	<%1

(Startup Conclave), 2016
Publicat ion

21	Perumal, B., M. Pallikonda Rajasekaran, and S. Duraiyarasan. "An efficient hierarchical attribute set based encryption scheme with revocation for outsourcing personal health records in cloud computing", 2013 International Conference on Advanced Computing and Communication Systems, 2013. Publicat ion	<%1
22	dblp.uni-trier.de Int ernet Source	<%1
23	www.ejournal.org.cn Int ernet Source	<%1
24	www.cis.umassd.edu Int ernet Source	<%1
25	documents.mx Int ernet Source	<%1
26	YaPing Chi. "An Improved Sealing Scheme for Trusted Storage", 2009 International Conference on Computational Intelligence and Software Engineering, 12/2009 Publicat ion	<%1
27	Aluvalu, RajaniKanth, and Lakshmi Muddana. "A Survey on Access Control Models in Cloud Computing", Advances in Intelligent Systems and Computing, 2015.	<%1

Publicat ion

28	docplayer.net Int ernet Source	<%1
29	www.ijoer.in Int ernet Source	<%1
30	Yan, Zheng, Xueyun Li, Mingjun Wang, and Athanasios Vasilakos. "Flexible Data Access Control based on Trust and Reputation in Cloud Computing", IEEE Transactions on Cloud Computing, 2015. Publicat ion	<%1
31	Gupta, Subham Kumar, Seema Rawat, and Praveen Kumar. "A novel based security architecture of cloud computing", Proceedings of 3rd International Conference on Reliability Infocom Technologies and Optimization, 2014. Publicat ion	<%1
32	Wei, Guiyi, Rongxing Lu, and Jun Shao. "EFADS: Efficient, flexible and anonymous data sharing protocol for cloud computing with proxy re-encryption", Journal of Computer and System Sciences, 2014. Publicat ion	<%1
33	Shaikh, Rizwana, and M. Sasikumar. "Data Classification for Achieving Security in Cloud Computing", Procedia Computer Science, 2015. Publicat ion	<%1

34	Ali, Mazhar, Samee U. Khan, and Athanasios V. Vasilakos. "Security in cloud computing: Opportunities and challenges", Information Sciences, 2015. Publicat ion	<%
35	Lecture Notes in Computer Science, 2009. Publicat ion	<%
36	Shimbre, Nivedita, and Priya Deshpande. "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES Algorithm", 2015 International Conference on Computing Communication Control and Automation, 2015.	<%