Open Access **Baghdad Science Journal** **P-ISSN: 2078-8665**
Published Online First: Suppl. November 2022 **2022, 19(6): 1445-1453** **E-ISSN: 2411-7986**

DOI: https://dx.doi.org/10.21123/bsj.2022.7281

Cloud Data Security through BB84 Protocol and Genetic Algorithm

Jaydip Kumar ***Vipin Saxena***

Department of Computer Science, BabasahebBhimraoAmbedkar University, Lucknow, India.
*Corresponding author: jaydipkumar2001@gmail.com
E-mails addresses:profvipinsaxena@gmail.com

Received 3/4/2022, Accepted 7/8/2022, Published Online First 25/11/2022, Published 5/12/2022

Abstract:

In the current digitalized world, cloud computing becomes a feasible solution for the virtualization of cloud computing resources. Though cloud computing has many advantages to outsourcing an organization's information, but the strong security is the main aspect of cloud computing. Identity authentication theft becomes a vital part of the protection of cloud computing data. In this process, the intruders violate the security protocols and perform attacks on the organizations or user's data. The situation of cloud data disclosure leads to the cloud user feeling insecure while using the cloud platform. The different traditional cryptographic techniques are not able to stop such kinds of attacks. BB84 protocol is the first quantum cryptography protocol developed by Bennett and Brassard in the year 1984. In the present work, three ways BB84GA security systems have been demonstrated using trusted cryptographic techniques like an attribute-based authentication system, BB84 protocol, and genetic algorithm. Firstly, attribute-based authentication is used for identity-based access control and thereafter BB84 protocol is used for quantum key distribution between both parties and later the concept of genetic algorithm is applied for encryption/decryption of sensitive information across the private/public clouds. The proposed concept of involvement of hybrid algorithms is highly secure and technologically feasible. It is a unique algorithm which may be used to minimize the security threats over the clouds. The computed results are presented in the form of tables and graphs.

Keywords: Attribute based Encryption, BB84 Protocol Cloud, Data Security, Geneticncryption/Decryption, Quantum Key Distribution.

Introduction:

During past years, technology is rapidly changing. Cloud computing is the most popular technique to store the user's or organization's information in a centralized manner and becomes a very classy technique in a few years. The standards of cloud computing are presented in the year 2006 by the National Institute of Standards and Technology (NIST) for the centralization of information that has locally/globally storage. Many of the organizations are trying to shift business over the cloud due to its faster availability, minimization of cost, and credibility of information but the data security is still not fully trustable. For providing security to the cloud data storage, the data owner stores the information in encrypted form which the cloud's users decide to access. For security purposes, the data owner provides a decryption key to the users to access the data. Before accessing the data from the centralized storage, the cloud user needs authentication permission if the cloud server is granted then access the information otherwise not. Cryptography is a Mathematical security technique that plays a vital role in the field of information security and it provides two types of security techniques such as symmetric which encrypts and decrypts with the same key and asymmetric cryptography which can encrypt or decrypt with different keys. The simple cryptographic technique is breakable and already reported in the literature. The available techniques of breaking security and breaching data from the cloud are very crucial. To avoid data leakage, there is a need to send encryption or decryption keys with different techniques to make cloud computing as secure and trustable. The authentication of the user, key generation, and encryption/decryption are three

major parts to secure the user's information and these parts should be more trustable and secure.

In the field of data security, quantum cryptography is an unbreakable security technique in the field of data security which is based on laws of quantum physics that play a vital role in network security. Quantum cryptography uses the photons to generate cryptographic keys and transmits to the receiver using a quantum channel. A quantum machine uses quantum theory to solve the traditional cryptographic Mathematical problems such as logarithmic, integer factorization problems, etc. To observe the quantum mechanical state without changing its quantum state, it is impossible to break quantum cryptographic algorithms. If any eyedropper wants to rewrite the quantum communication states between the sender and receiver, it can be traced normally by the quantum systems. In the series of data security, authentication is the first step to providing cloud data security. Attribute-based authentication is an attribute of a user's property applied for access control as predicates. Cloud computing provides highly secure encrypted data to store over the cloud server. The traditional cryptographic technique fails to secure data. To avoid this, genetic encryption algorithm is also used to encrypt cloud data in terms of DNA sequence. The genetic data uses the gene for generating the DNA sequence. The DNA sequence contains nucleic acid which contains the genetic information. It has four nucleotide bases which are Adenine (A), Cytosine (C), Thymine (T), and guanine (G).

In the present work, two important challenges are covered and these are related to security key which is not enough to avoid data leakage in cloud computing and another is secret key sharing in which network communication system is not fully trustable for cloud user to keep personal or professional data in secure form.

By the use of proposed framework, unauthorized users or intruders can be discarded to access the cloud data and it prevents data leakage during transmission over the network. The framework is used to

- Propose an access control system using the attribute-based authentication system to enhance the security parameter;
- Propose a secure secret key transmission using BB84 protocol known as quantum key distribution to avoid the leakage of secret key sharing;
- Propose encryption/decryption of cloud data through the genetic algorithm.

Therefore, a hybrid security framework for cloud computing data is proposed and for unsecure channel, attribute-based authentication is employed for access control, and quantum key distribution is used for secret shearing between sender and receiver. To share the secret key, the suggested framework employs a quantum key distribution mechanism in which data owner encrypts the information before sending it to the data user. To outsource cloud data, the DNA based genetic algorithm is used to encrypt data. After properly authenticating, the data user receives the data after conducting partial decryption. To obtain the original data, the data user uses the shared secret key. Some of the important references are described in the next Section 2 from which it is observed that combination of BB84 protocol with concepts of genetic algorithm are not available in the literature and on this aspects, proposed framework is described in the Section 3. The framework is implemented or tested in the Section 4 and last Section 5 presents the concluding remarks and directions to extend the present work.

Related Work:

Many different researchers have focused research on the improvement of cloud data security. Quantum cryptography offers unconditional security based on the principles of quantum computers. The authors reviewed and implemented a well-known branch of quantum cryptography which includes theory and implementation such as quantum key distribution [1].

A study of quantum cryptography and its application such as encryption and key distribution is used for avoiding the access control problem. The author proposed an encryption technique and key distribution protocol for the Categorical Quantum Mechanics (CQM) for the graphical language for CQM [2]. In the twenty-first century, identity-based theft is the most risky in cybercrime, and the numbers of hackers are increasing day by day in exponential manner. The quantum cryptography is used to provide the security and confidentiality for the network security. The authors implemented a model which uses identity-based authentication and used to confirm the user's identity before getting access and also used quantum identity-based authentication and BB84 protocol for securing the cloud data [3].

In the field of mobile cloud computing, quantum cryptography also plays an important role in the security of mobile cloud data. Quantum key distribution for cloud mobile users using two phases is proposed by the multiplexing technique used for the transformation of the quantum distribution network using the classical optical network. It is also used an authentication protocol for access

control and then quantum keys are transferred to the cloud mobile user's storage area and the mobile user can easily access the storage area through the quantum secret key. All the experiments are performed using the real quantum cryptography environment which proves the validity of quantum cryptography for mobile cloud computing [4].

There are several traditional cryptographic techniques which failed with respect to confidentiality and integrity across the world wide network. The author implemented a model on the AVISPA which provided confidentiality in the presence of an attacker and also compared it with the existing cryptographic techniques [5]. Verifiable quantum computation resolves the problem of authentication and privacy based while cloud computing clients interact with the quantum computers. Li et al.[6] implemented a model based on a cryptographic calculation which is used for distributed structure of cloud computing, and used cluster state with grid distributed manner and the random key is always used by the cloud client which builds trust for the confidentiality to the users. Winick et al. [7] proposed a safe, effective, and hard-grained numerical computation method for generating key rates using Quantum Key Distribution (QKD) protocols, and interpreted by generating higher key rates in comparison to other research.

Cloud computing needs a visible solution for securing computing resources.The current security technique has a certain presumption which may be break with few efforts. To provide high security for cloud storage has made using the quantum cryptography which is an unconditional security technique. The author implemented and proposed a new security model based on the BB84 protocol for data distribution which is more beneficial for providing security to cloud data storage and also consider cloud servers, owner, and clients. This technique provided secure communications using the proposed model and provides a comparative study of the success and failure rate of public and private clouds [8].

Cloud computing has become a more promising technology in the field of information technology so the protection of cloud data is more important. The theft of identity authentication is the more serious concern of cloud computing so the author proposed a novel security protocol for authenticating the user through quantum cryptography [9].

In the public and private cloud storage accessibility, availability, and cost-effectiveness are the most important factors of the cloud environment. The transmission of information is the biggest concern of the cloud and is still not safe as a result of this aspect many cloud user's loss their personal information. Olanrewajuet al.[10] proposed a novel security technique that is an integrated service of advanced quantum cryptography with cloud computing. Access authentication is the decidable property of cloud computing that decides the cloud user's access. Qiu L et al.[11] investigated quantum cryptography to develop access control and used BB84, identity authentication, and digital certificate protocols for cloud data security. The data is growing in exponential order and security breaches are also increasing, and the difficult part for cloud providers provides security to users. The author proposed a Mathematical model for generating encryption and decryption of data. For the encryption, an encrypted message may clone three layers, and all the three layers sum up and generatedstrongerciphertext for the message [12].

Cloud computing changed the working style in the recent era of technology. It is an emerging technology that is rapidly changing technology for providing security and getting attention every time, and different large organizations are showing interest and shifting data in cloud storage because cloud storage has a unique property that attracts more organizations due to its flexibility of storage capacity. A novel security model has been proposed based on a DNA encryption algorithm which crops the security of cloud storage [13]. The DNA sequence with cloud computing storage is also used for the medical treatment of a patient. Wang et al. [14]presented a method to store patient information related to deceases and biological information in cloud storage and identify patients with biological sequence, so the doctor easily identifies patient's past checkups and medicines and suggests medicines according to past medical information and present condition of the patient.

From the compilation of the above research papers contributed by the researchers, it is observed that cloud computing security requires advanced technological solutions to avoid leakage of secrete keys and previouslyproposed security solutions took a very long time to encrypt and decryptand were not long-lasting when large amounts of private personal information were kept in cloud computing.So, there is need to propose a new model which can reduce computational complexity and provide safe and secure cloud computing environment in the presence of hackers and intruders available on the network. It is further investigated that in the present scenario, combination of BB84 protocol with genetic based encryption/decryption called as BB84GA protocol is more powerful technique in

comparison of other existing security techniques. The proposed model is described in the next Section 3.

Proposed Methodology

1. Quantum Cryptography

Let us first describe quantum cryptography which is the prime technology in the field of network security which provides secure communication between two sender and receiver using the quantum physics theory. Quantum cryptography was first presented by Stephen Wiesner in the year of 1970's. Charles H. Bennett from the IBM and Gilles Brassard of the University of Montreal collaborated with Stephen and proposed Quantum Key Distribution (QKD)known as BB84 protocol in the year 1984 [15]. One of the most important techniques of quantum cryptography is the BB84 protocol, which use the quantum light of physics property to provide unconditional security and privacy to the classical information [16]. Quantum communication uses free space, especially with a satellite attack that occurred it could be detected by the classical channel monitoring technique, and a simplified protocol and hardware system of quantum communication could be realized and deliver an improved key rate [17].

The analysis of quantum key distribution protocol consists of Ram sending a sequence of single qubits, which is the combination of randomly selected states $\{|\uparrow\rangle,|\rightarrow\rangle,|\nearrow\rangle,|\searrow\rangle\}$and Shyam chooses its measurement based on random choice, interacts for the basic choice for every encoded qubit, intruder attack detection performed by comparison of measurement results based on fraction on their choices if match then successful otherwise attack detected between Ram and Shyam, the quantum computing produces a sequence of maximally entangled states (|00> + |11>) /$\sqrt{2}$, and Ram and Shyam measuring their random choice of bases [18].

The quantum key distribution uses the different polarization of quantum states and it is used to secure transmission between the Ram and Shyam which is described below:

- Ram generates random sequence of bits and sends to Shyam;
- Shyam received photons and decodesthe received sequence them randomly;
- Both Ram and Shyam compare these bits which have same basis. If the estimated rate is less than the considered, test is successful.
- At last both parties such as Ram and Shyam compare these bits which have the same basis, because estimated rate is less so test is successful [8].

Key exchange using Quantum channel is shown below in Table 1.

Table 1. Key Exchange Using Quantum Channel (8)

Alice String	1	1	0	1	0	0	1	0	1	1	1	1	0	0
Alice basis	+	+	+	X	X	+	X	X	X	X	+	+	+	+
Alice send	-	-	|	\	/	|	\	/	\	\	-	-	|	|
Bob's basis	+	X	+	+	X	+	X	+	X	X	+	+	+	+
Bob's String	1	0	0	1	0	0	1	1	1	1	1	1	0	0
Same Basis?	Y	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Bits to keep	1		0		0	0	1		1	1	1	1	0	0
Test	Y		N		N	Y	N		N	N	N	Y	Y	N
Key			0		0		1		1	1	1			0

2. Genetic Algorithm

Further the concept of genetic algorithm uses the theory of Charles Robert Darwin's evolution. The idea behind the genetic algorithm is to replicate nature as individual population adapted environment in terms of the natural selection process and the behavior of the natural system. It needs to initialize the population according to suitability and selection of fitness function which is important for getting a suitable outcome and hereafter used three operations to the transformation of the population (Chromosomes) into new population with better fitness [19]. Genetic algorithm has mutation operator whichis used to preserve diversification from one generation of a population of genetic algorithm chromosomes to the next.Crossover operator is used for the combination of genetic information of two parents for generating a new offspring[20]. Selection selects individuals at random from the current population to be parents and uses it to provide the children for the next generation[21].

The genetic algorithm is the combination of four nuclear bases such as adenine (A), guanine (G), cytosine(C), and thymine (T)[22]. The combination of these bases forms a code that describes genetic information and these sequences are used to enhance data security each base pair is related and shown In Table 2. The obtained binary digits of

sequence are used as a key for decoding the user's information [23].

Table 2. DNA Sequence Table[20]

DNA Sequence	Binary Sequence
T	00
A	01
G	10
C	11

3. Attribute Based Authentication

In the current technological world, access control is the most prominent security technique to get secured cloud data and provides the controllable manner of user's information. The control of the system provided resource-based permission to get access[24]. On behalf of the user attribute, the resource attribute is provided by the data owners where the attribute can be any information such as the user's job functions and resource quality and access control permission which is relevant for getting access to users and avoiding unauthorized access[25]. The Attribute-based frameworks are a characteristic fit for settings where the roles of the clients rely upon the combination of attributes. Using this system, the user obtains a combination of multiple attributes from authorities, and the user's accessibility depends on their attributes[26].

Proposed Framework

A scheme for authenticating a user is proposed for secure cloud data transmission over the network using attribute-based authentication, quantum key distribution, and a genetic algorithm for data encryption and this proposed scheme is called as BB84GA. In the first step attribute-based authentication is used for authentication of a cloud user's attribute and quantum key distribution is used for key generation for the encryption and decryption using photon polarization states to transmit information over the network for the secure transmission of user's data and finally, genetic algorithm is used for encryption of information. The different algorithms are hybrid according to following steps:

Algorithm-1

Attribute_Based_Authentication() {

- *Let* U *be the Universal Set of possible attributes;*
- *Assign a set of attributes* A ⊆ U*to* Ram;
- Shyam*has its own set of attributes*A′ ⊆ U;
- *Verify* |A ∩ A'|=n *and* n ≥ r *where* r *any real number if satisfy the condition then get forward otherwise reject it*}

After satisfying the Algorithm-1, key generation will start according to following:

Algorithm-2

Key_Generation(){

Step 1: *Ram generate any Binary sequence a*
For i in a
$R_b[i]$=*Random_basis(a[i])*
$P_1[i]$= *Polarized_photons*($R_b[i]$)
Ram sends P_1 *to shyam through quantum channel*
Step 2:*Shyam Received polarized photons* P_1 *from Ram*
For j in P_1
$R_b[j]$ = *Random_basis*(P_1)
P_2= *Polarized_photons*($R_b[j]$)
Both Ram and Shyam compare polarized photons in classical channel and check $P_1 \cap P_2 = x$ *where x is the selected key for encryption and decryption.*
}

Algorithm-3

Encryption()
$\{Cipher = ENC_{DNA}(Message, x);\}$

Algorithm-4:

Decryption ()
$\{Message = DEC_{DNA}(Cipher, x);\}$

Where DNA represents the encryption and decryption are based upon the concepts of genetic algorithm. The proposed framework is given below in following Fig.1.

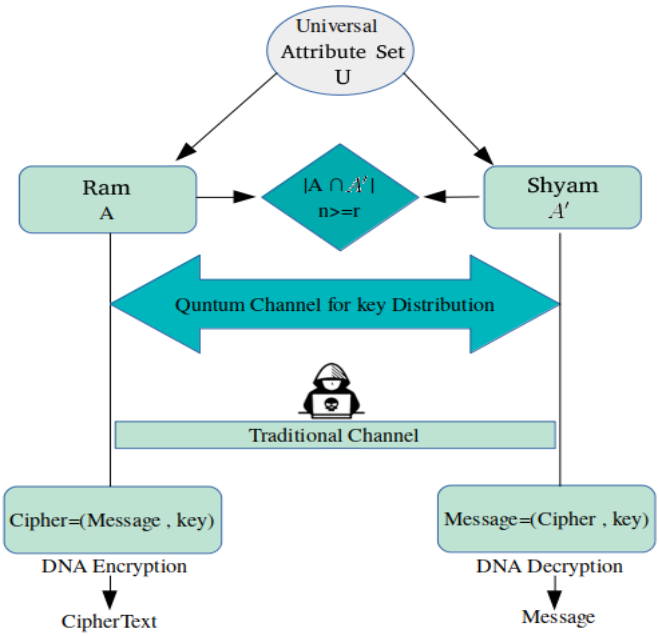

Figure 1. Proposed framework for Cloud Data Encryption

Results and Discussion:

The experimental evaluation of the proposed work as shown in above fig. 1 extends the security of cloud computing using different trusted techniques. Attribute-based authentication for authenticating the cloud user's identity and BB84 protocol for establishing the secure channel for key transformation using quantum channel and then DNA genetic technique for the encryption and decryption of cloud user's sensitive information are applied. The proposed BB84GA algorithm is implemented using Python 2.7.17 and Avita-Liber machine of intel Core i5-10210U CPU@1.60GHz × 8, 8GB of memory, 256 GB SSD installed on 64-bit instruction set kernel Linux (Ubuntu 20.04.3 LTS) OS is used for uploading and downloading the data from the cloud.

Let's take an example,Ram wants to send a message like ***"WELCOME TO BBAU LUCKNOW"***toShyam. Before sending message Ram set a set of attributes for Shyam, if Shyam related to ABC department of XYZ Company then Shyam able to decrypt message using shared key. Ram generate secrete key such as [94, 2, 175, 117, 66, 26, 163, 3, 158, 20, 245, 28, 100, 130, 209, 11, 212, 58, 65, 172, 97, 127, 134, 16, 40, 40, 204, 1, 191, 241, 145, 30] using BB84 protocol and send with quantum channel to Shyam. Now if Shyam satisfy the set of attributes then able to decrypt message using received key. The whole process of the proposed algorithm takes computation time of "58 Millisecond". The results of the proposed frameworkare given below in Fig. 2:

```
(base) dcs@dcs-NS14A8:/media/dcs/New Volume/QuantumwithGenetic$ python3 DNAquantum.py
Message:  WELCOME TO BBAU LUCKNOW

attribute matched successfully

Shyam's shared key: [94, 2, 175, 117, 66, 26, 163, 3, 158, 20, 245, 28, 100, 130, 209, 11, 212, 58, 65, 172
, 97, 127, 134, 16, 40, 40, 204, 1, 191, 241, 145, 30]

Ram's shared key: [94, 2, 175, 117, 66, 26, 163, 3, 158, 20, 245, 28, 100, 130, 209, 11, 212, 58, 65, 172,
97, 127, 134, 16, 40, 40, 204, 1, 191, 241, 145, 30]

Successful key exchange! Keys match.
==========================encryption==================================

DNA-GET is running...

Final DNA sequence: GTCATCCTCGGTTCCCCGAGCGCCTTTGGTCGAAATAGGAAAGCAGTTCACCCTTAGACCTATGGAGTATCAGAGTCCTCCTAAAAC
CAAGC
==========================decryption==================================

DNA-GDT is running...

Decryption Message: WELCOME TO BBAU LUCKNOW
Total execution time in millisec: 58
```

Figure 2. Results of Proposed Framework on String "WELCOME TO BBAU LUCKNOW"

A collection of 5 datasets is considered as D1, D2, D3, D4, and D5 which contained general text with different sizeswhich is presented in the Table 3. The proposed experiments are repeated

multiple times with each dataset and captured the computation time to compare the experiments.

The execution time for all algorithms is recorded in milliseconds. Moreover, the throughput efficiency is also calculated as bytes per second for both encryption and decryption, and the efficiency behavior of both encryption and decryption processes are also observed during the experimental evaluation of the dataset and compared with different algorithms such as DES, 3DES, RSA, Blowfish, AES, CryptoGA with proposed BB84GA algorithm. Fig. 3 and Table 4 show the average encryption and decryption time of executions for large datasets, respectively. The results analysis show that the proposed model BB84GA takes less time as compared with other algorithms [27].

Table 3. Representation of Datasets

S. No.	Dataset	Size in Byte
D1	**General Text**	**54**
D2	**General Text**	**205**
D3	**General Text**	**213**
D4	**General Text**	**1012**
D5	**General Text**	**1059**

Table 4. Comparison of Computation Time of Present Framework

	D1	D2	D3	D4	D5
AES	186	93	185	203	341
DNA	29	52	58	105	198
DES	49	63	76	97	113
CryptoGA	29	37	54	82	144
Present Framework (BB84GA)	18	33	28	64	110

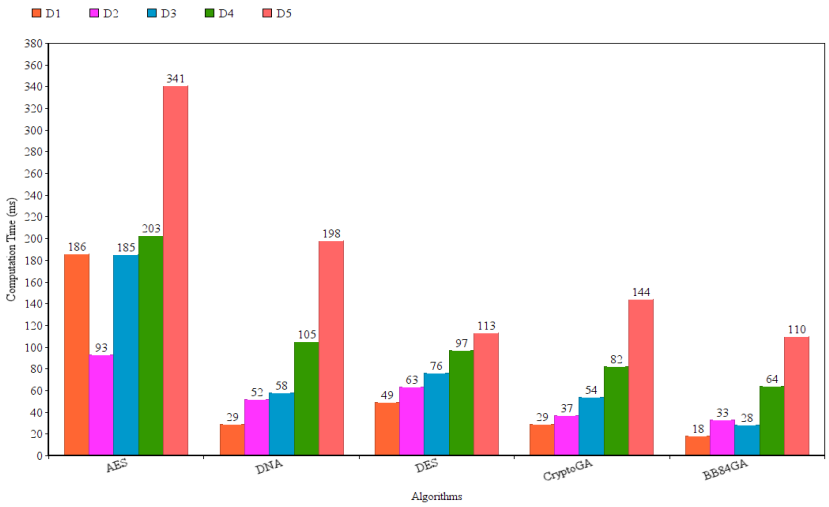

Figure 3.Comparison Graph BB84GA v/s Methods in [27]

Conclusions:

In addition to the contributions of our previous work, the above BB84GA framework is based on both quantum and classical cryptography models which effectively enhanced the privacy of cloud user's data transmission from the cloud server to the local computer through encrypted cloud data. A successful data transmission uses three stages first user authentication, second data encryption, and final data transmission if all these three stages are secure then the cloud provider is trusted. So existing classical key distribution techniques are upgraded to quantum key distribution techniques which uses the theory of quantum light to provide secure key transmission over the secure channel. User authentication is performed using attribute-based authentication and cloud data is encrypted using a genetic algorithm through the quantum key. The proposed BB84GA algorithm is secure and fast in comparison with the other existing security techniques.

In the above work, a unique quantum security technique is applied that generates keys based on quantum lights which are used for cloud data masking to increase the security over the communication channels. Furthermore, the proposed method also improves user access control security and data privacy while accessing the cloud data. The limitation of present research article is depending upon the technology, key sharing, and personal or professional data size of the user used in cloud computing. Future work of present research is to improve the population of genetic sequence to prevent the local minima as well as enhance the

fitness function to improve the security of cloud computing data storage.

Acknowledgment:

One of the authors i.e. Jaydip Kumar is grateful to the University Grants Commission, New Delhi for providing Junior Research Fellowship to carry out the present research work in excellent computational environment in the Babasaheb Bhimrao Ambedkar University, Lucknow, India.

Authors' declaration:

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are mine ours. Besides, the Figures and images, which are not mine ours, have been given the permission for re-publication attached with the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee in BabasahebBhimraoAmbedkar University.

Authors' contributions statement:

J. K. contributed to the design and implementation of the research, to the analysis of the results and to the writing of the manuscript. V. S. performed the computation sand verified the analytical methods. All authors discussed the result sand contributed to the final manuscript.

References:

1. Zhang H, Ji Z, Wang H, Wu W. Survey on quantum information security. *China Comm*. 2019 Oct; 16(10): 1-36.
2. Zhou L, Wang Q, Sun X, Kulicki P, Castiglione A. Quantum technique for access control in cloud computing II: Encryption and key distribution. J NetwComput Appl. 2018 Feb 1; 103: 178-84.
3. Sharma G, Kalra S. Identity based secure authentication scheme based on quantum key distribution for cloud computing. Peer PeerNetw Appl. 2018 Mar; 11(2): 220-34.
4. Han J, Liu Y, Sun X, Song L. Enhancing data and privacy security in mobile cloud computing through quantum cryptography. In 2016 7th IEEE I Conf on Soft Eng and Service Sci *(ICSESS)* 2016 Aug 26: 398-401. IEEE.
5. Mustafa I, Khan IU, Aslam S, Sajid A, Mohsin SM, Awais M, et al. A lightweight post-quantum lattice-based RSA for secure communications. *IEEE Access*. 2020 May 19; 8: 99273-85.
6. Li J, Zhao Y, Yang Y, Lin Y. Verifiable Quantum Cloud Computation Scheme Based on Blind Computation. IEEE Access. 2020 Mar 19; 8: 56921-6.
7. Winick A, Lütkenhaus N, Coles PJ. Reliable numerical key rates for quantum key distribution. Quantum. 2018 Jul 26; 2:77.
8. Murali G, Prasad RS. CloudQKDP: Quantum key distribution protocol for cloud computing. In2016 I Conf on InfComm and Emb Sys. 2016 Feb 25: 1-6. IEEE.
9. Fatima S, Ahmad S. Quantum key distribution approach for secure authentication of cloud servers. Int J Cloud App Comp. 2021 Jul 1; 11(3): 19-32.
10. Olanrewaju RF, Islam T, Khalifa OO, Anwar F, Pampori BR. Cryptography as a service (CaaS): quantum cryptography for secure cloud computing. Indian J Sci Technol. 2017 Feb; 10(7): 1-6.
11. Qiu L, Sun X, Xu J. Categorical quantum cryptography for access control in cloud computing. Soft comput. 2018 Oct; 22(19): 6363-70.
12. Matthews RA. The use of genetic algorithms in cryptanalysis. *Cryptologia*. 1993 Apr 1; 17(2): 187-201.
13. Sugumar R, Leelavathy L. Ensure Data Security and Privacy using DNA Symmetric Encryption Method in Cloud. J InfComput Sci. 2020; 10(3): 676-689.
14. Wang B, Song W, Lou W, Hou YT. Privacy-preserving pattern matching over encrypted genetic data in cloud computing.IEEEIntConfIntell. ComputCommun. 2017 May 1: 1-9. Doi:10.1109/INFOCOM.2017.8057178
15. Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. Rev Mod Phys. 2002 Mar 8; 74(1): 145.
16. Li J, Li N, Zhang Y, Wen S, Du W, Chen W, et al. A survey on quantum cryptography. Chinese J Electron. 2018 Mar; 27(2): 223-8.
17. Wang L, Alexander CA. Quantum science and quantum technology: Progress and challenges. Am. J. Electr. Electron. Eng. 2020 Mar 27; 8(2): 43-50.
18. Broadbent A, Schaffner C. Quantum cryptography beyond quantum key distribution. Des Codes Cryptogr. 2016 Jan; 78(1): 351-82.
19. Javurek M, Turčaník M, Matej B. Model of Encryption System with Genetic Algorithm. In 2019 Communication and Information Technologies (KIT*)* 2019 Oct 9 : 1-5.
20. Yadav M, Breja M. Secure DNA and Morse code based Profile access control models for Cloud Computing Environment. ProcediaComput Sci. 2020 Jan 1; 167: 2590-8.
21. Wu Y, Wei Z, Deng RH. Attribute-based access to scalable media in cloud-assisted content sharing networks. IEEE Trans Multimedia. 2013 Jan 10; 15(4): 778-88.
22. Maji H, Prabhakaran M, Rosulek M. Attribute-based signatures: Achieving attribute-privacy and collusion-resistance. Cryptol. 2008: 1-23: https://eprint.iacr.org/2008/328
23. Kumar J, Saxena V. Hybridization of Cryptography for Security of Cloud Data.Int J Future Gener. Commun. Netw. 2020; 13(4): 4007-14.
24. Kumar J, Saxena V. Asymmetric encryption scheme to protect cloud data using paillier-cryptosystem.Int J ApplEvolComput. 2021 Apr 1; 12(2): 50-8.
25. Kumar S, Kumar N. Conceptual Service Level Agreement Mechanism to Minimize the SLA Violation with SLA Negotiation Process in Cloud

Computing Environment. Baghdad Sci J.2021 Jun 20; 18(2 (Suppl.)): 1020.
26. Abed MM, Younis MF. Developing load balancing for IoT-cloud computing based on advanced firefly and weighted round robin algorithms. Baghdad Sci J. 2019; 16(1):130-139.
27. Tahir M, Sardaraz M, Mehmood Z, Muhammad S. CryptoGA: a cryptosystem based on genetic algorithm for cloud data security. Cluster Comput. 2021 Jun; 24(2): 739-52.

أمن البيانات السحابية من خلال بروتوكول BB84 والخوارزمية الجينية

جايديب كومار **فيبين ساكسينا**

قسم علوم الحاسوب، جامعة باباصاحب بهيمرو أمبيدكار، لكناو، الهند.

الخلاصة:

في العالم الرقمي الحالي، أصبحت الحوسبة السحابية حلاً ممكناً لإضفاء الطابع الافتراضي على موارد الحوسبة السحابية. بالرغم من أن الحوسبة السحابية تتمتع بالعديد من المزايا للاستعانة بمصادر خارجية لمعلومات المؤسسة ، إلا أن الأمان القوي هو الجانب الرئيسي للحوسبة السحابية. سرقة مصادقة الهوية أصبحت جزءًا حيويًا من حماية بيانات الحوسبة السحابية. في هذه العملية ، ينتهك المتسللون بروتوكولات الأمان وينفذون هجمات على المؤسسات أو بيانات المستخدم. إن الإفصاح عن البيانات السحابية يؤدي إلى شعور مستخدم السحابة بعدم الأمان أثناء استخدام النظام الأساسي السحابي. لا تستطيع تقنيات التشفير التقليدية المختلفة إيقاف مثل هذه الأنواع من الهجمات, بروتوكول BB84 هو أول بروتوكول تشفير كمي تم تطويره بواسطة بينيت وبراسارد في عام 1984. تم في هذا البحثإثبات ثلاث طرق لأنظمة أمان BB84GA باستخدام تقنيات تشفير موثوقة مثل نظام المصادقة القائم على السمات ، وبروتوكول BB84 ، والخوارزمية الجينية.أولاً ، يتم استخدام المصادقة القائمة على السمات للتحكم في الوصول المستند إلى الهوية وبعد ذلك يتم استخدام بروتوكول BB84 لتوزيع المفتاح الكمي بين كلا الطرفين ، وفيما بعد يتم تطبيق مفهوم الخوارزمية الجينية لتشفير / فك تشفير المعلومات الحساسة عبر السحابات الخاصة / العامة.المفهوم المقترح لمشاركة الخوارزميات الهجينة آمن للغاية ومجدي من الناحية التكنولوجية. تعتبر هذهالخوارزمية فريدة من نوعها يمكن استخدامها لتقليل التهديدات الأمنية عبر السحب. النتائج المحسوبة معروضة في شكل جداول ورسوم بيانية.

الكلمات المفتاحية: التشفير المستند إلى السمات، بروتوكول BB84، أمان البيانات السحابية، التشفير الجيني / فك التشفير، توزيع المفتاح الكمي.