Biometric Encryption in Cloud Computing: A Systematic Review

Mehreen Ansar[1], Muhammad Sheraz Arshad Malik[2], Mubeen Fatima[3], Sadaf Aslam[4], Anum Rasheed[5], Iqra Nazir[6]

Department of Computing, Riphah International University, Faisalabad, Pakistan
[2]Department of Information Technology, Government College University, Faisalabad, Pakistan
[3]SEECS, National University of Science and Technology, Islamabad, Pakistan

Summary
This Review paper is about the security of bio metric templates in cloud databases. Biometrics is proved to be the best authentication method. However, the main concern is the security of the biometric template, the process to extract and stored in the database within the same database along with many other. Many techniques and methods have already been proposed to secure templates, but everything comes with its pros and cons, this paper provides a critical overview of these issues and solutions.

Key words:
Cloud Computing, Biometrics, Cloud Databases, Cryptography, Quantum Cryptography, Cognitive Cryptography, DNA Storages

1. Introduction

Basic Objective of this review paper is to safely store and retrieve the biometric templates inside the Cloud Data bases.
Cloud Computing is an IT paradigm that enables access to one common pool of configured systems and provide higher-level of services with minimal effort. Cloud security is a data set of policies, technologies and rules to protect data, applications, and the infrastructure of cloud computing. Mostly enterprise use cloud to store and maintain large data. Cloud security has become a concern for both cloud users and providers. Traditionally authentication like key generation, passwords, mostly encryption mechanism has failed making data insecure from intruders and black hat hacker.
Biometrics is the technical term for calculating and measuring different body parts by relating metrics to human characteristics. Biometrics authentication is used to control realistic identification and is unique for every person or individual. With increase demand of security, I recommend at using biometrics for the authentication process at cloud level. Biometrics is a combination of feature extractor, sensors and matching parts or modules which implements recognition algorithms on particular biometric pattern. The sensor works by scanning the biometric trait and give output in digital form. The check and control is done to ensure that the output sample is reliable and safe for feature extraction and matching modules

Now, authentication and verification are considered as the most important goals to be fulfilled for the physical world (the world to live in) or the virtual world (Internet). Different techniques exist to authenticate and verify the user such as passwords, smart cards, pins, and other authentication tokens which include biometrics like finger prints, a retina, iris, facial expressions, voice, signatures and face.
Among all the authentication techniques present because of the uniqueness biometrics is considered as the most reliable authenticators.
Biometric cryptosystem, as the name suggest, take the original template and give out the encrypted template which reveals the least amount/zero percent of information about the original template. Due to this characteristic, the security of such systems is said to be high.
Basic biometric Authentication:
The above diagram is depicting the basic authentication process of template extraction, matching and storing.

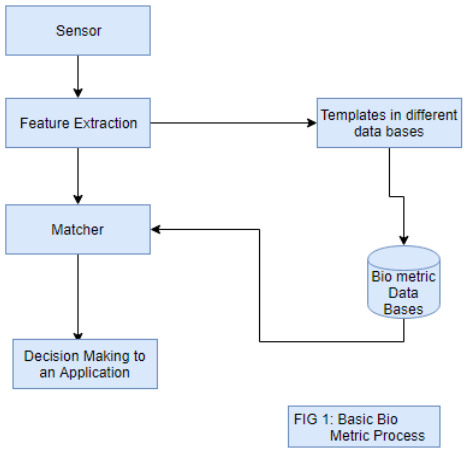


Fig. 1 Basic Biometric process.

Consist of four basic steps:

- Sensors : To detect biometric
- Signal processing:Clear feature extraction
- Pattern Matching: Closely matched to the original template.
- Decisions: True or false match

Manuscript received August 5, 2018
Manuscript revised August 20, 2018

- These steps are used to extract and store the biometrics free of noise and signal losses.It should be complete and secure to be stored in the database by discarding unclear and ambigious or clone templates.Biometrics are used to prevent third party attacks, unauthorized means and provide valuable confidence among the individuals.

Authentication and verification are considered as the most important goals to be fulfilled for the physical world (the world to live in) or the virtual world (Internet). Different techniques exist to authenticate and verify the user such as passwords, smart cards, pins, and other authentication tokens which include biometrics like finger prints, a retina, iris, facial expressions, voice, signatures and face. Among all the authentication techniques present because of the uniqueness biometrics is considered as the most reliable authenticators.

Biometric cryptosystem, as the name suggest, take the original template and give out the encrypted template which reveals the least amount/zero percent of information about the original template. Due to this characteristic, the security of such systems is said to be high. To prevent our biometric templates we use various techniques to save in a secure manner and detect error if any.

Techniques for error-correcting code are

- fuzzy vault scheme (Integers)
- fuzzy commitment scheme (bits of string)

Usage of keys include

A key-binding biometric cryptosystem is a secret key and the biometric data is connected with a reference template to generate helper data. Helper data is the public data to store the biometric template by removing variations and hiding the original template.

A key-generation biometric cryptosystem, the key is generated from the biometric itself and don't need any extra cryptographic key to secure the template. There is no issue of the key security yet generation of a stable cryptographic key in the presence of intra-class variations exists. The Quantization process has also been employed in the various key generating techniques to remove the intra-class variations during the key extraction process.

This paper is being classified as Section II and III dedicates for related work Section IV provides us a proposed solution for this paper and Section V concludes the effort of this review paper

2. Tables

Table 1: Biometric Issues and Future work

S No.	Year	Proposed Algorithms	Pros	Future Work
1	2018	Novel Biometric Inspired Homomorphic Encryption Algorithm (Bihea)	Encrypts the user information at run-time	Real test with distributed computing
2	2018	Biometrics-as-a-Service (BaaS) continuous innovation is encouraged	Execution and rendering micro payments to the correspondi ng developer	Need of Optimal matching algorithm selection
3	2018	Advanced Minutiae Base Algorithm (AMBA) +Advance Encryption Standard (AES) algorithm	Usage of multi model authenticati on with one biometric technique	Need to use scheme with more than one biometric technique.
4	2018	Multimodal authenticati on system	Using biometrics for the edge centric cloud	Need to generate the secret key to enhance the security
5	2018	Splitting and distributing secret parts using cognitive cryptograph y techniques	Manage strategic information	Semantic interpretation of personal traits using non-standard bio metric specifications
6	2018	BEBA (Biometric encoding and Biometric authenticati on)	Blowfish has been used in data protection and key safety managemen t	one time passwords and level of encryption can be enhanced
7	2017	effective security patch to Cloud BI	secure against enrollment-level attackers	Can be made efficient for random value
8	2017	Biometric data Encryption and Matching algorithms	High level of privacy Protection	Can be tested with matrix value items
9	2017	Bio-hashing	Multi-cloud-server with Biometrics + ECC.	Can be evaluated for simulation in real-world environment
10	2017	Biometric Authenticati on	Reduces threat and load on resources	Secure Privacy for biometric authenticatio n is required

3. Literature Review

This section of Literature Survey is related to some important modules, algorithms and facts of Biometric Authentication on the basis of author analysis.

The author has introduced a novel biometric inspired homomorphic encryption algorithm (BIHEA) for securing data transmission of files in cloud at the hybrid level. Algorithm encrypts all the user data by providing unique one-time password and help against phishing and shoulder surfing. [1]

The author proposed a Biometrics-as-a-Service (BaaS) framework to perform biometric matching in cloud devices for providing privacy and security. The author used Linux-based virtual machine environment for fake logging and data theft to authenticate the cloud. [2]

In this paper the author introduced a biometric authentication with encryption and compression of data. For providing security Advanced Encryption Standards algorithm is used generate the secret key with its feature extraction from fingerprint biometrics using algorithm named as Advanced Minutiae Base Algorithm (AMBA). In the end the secret value is encrypted with generated biometric key using Advanced Encryption Standard (AES) Algorithm. [3]

In this paper, author use multi model authentication using one biometric technique. He proposed a model based on Advanced Minutiae Base Algorithm (AMBA) and Advance Encryption Standard (AES) algorithm, which reduces the computational load on the cloud and securing identity of the person by disclosing or decrypting with the relevant / same secret key. [4]

The author discussed cognitive cryptography to secure data by splitting it among different groups of trustees. Most of the safety problems are associated with authentication and information protection with respect to cloud security alliance (CSA). [5]

The author introduced a new protocol, BEBA (Biometric encoding and Biometric authentication) to overcome all the security problems in cloud surroundings. In BEBA protocol, identity verification has been combined with template protection in conjunction with completely different and powerful (RC4, RSA, AES and 3DES) encryption algorithms for accumulated safety. Blowfish has been used in data protection and key safety management. [6]

The author proposed the security of Cloud Biometric identification and proved how vulnerable it could be against enrollment-level attackers. The security assumption of Cloud BI does not capture attacks, like unauthentic user on to databases. He designed the attack model and showed how an attacker enrolls and exploits in order to recover authentic finger code. [7]

The author proposed a cloud identification model for outsourcing storage by utilizing matric and perturbed terms. First, the correctness of biometric identification is achieved. Secondly, privacy and efficiency of the biometric identification scheme is guaranteed against Level II and Level III attacks. [8]

The author proposed bio hashing and elliptic curve cryptography for the multi-server cloud for securing cloud biometric authentication and also allowing ECCbased protocols from Diffie-Hellman. [9]

The author proposed enrolment and verification process in Bio AaaS reduces the threat of data theft and reduces the load on resources. The template is then stored and encrypted using Reverse Circle Cipher algorithm and Pearson's formula. If the value comes closer to 1 than the two templates are considered same and the user is considered authenticated and allowed log in credentials to the cloud. [10]

According to the above table

Major problems lies in

- Exact matching of templates.
- A Real time implementation of data due to software and hardware cost.
- Security concerns while storing and extracting the templates
- Moving template from device to the database
- Generation of secret keys
- Middle man Attacks
- And Future goals may be concerned with
- Maintaining standards
- Securing Biometrics while Ageing ,Illness or Injury
- Controlling Environmental conditions, proper user training and usability factors.
- Increasing security level
- Increasing storage level

As big data owners are willing to preserve privacy by making use of user data in the form of biometric information by encrypting to the cloud databases to enroll and identify users by decrypting.

Apart from various problems and solutions disused in this review paper, in the future, more complex architecture and the beneficial statistical evidences should be studied. Let us have a look on its pros and cons

Pros

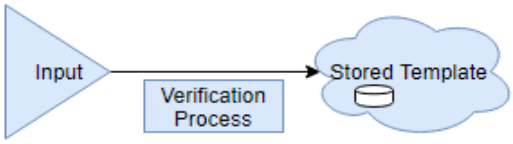
It's hard to fake because of uniqueness.
It provides convenience while applying passwords.
It's stable and changes very little in whole life.
It provides strong authentication and accountability.
Templates are non-transferable, less time consuming and more security required for identification may be less than five seconds.

Cons

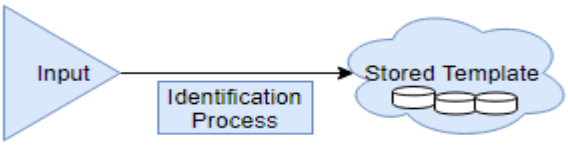
Authenticity of a biometric is captured and mapped to specific identity.
Lack of accuracy and privacy in retrieving data and saving can lead to system failure.
Error in biometric device i.e. false rejects and false accepts.
High cost in maintaining, integrating the systems up and running and also storing and saving biometrics.
It's not for physically disabled persons.

4. Proposed Solution

Depending on the need Biometric is all about person verification and identity.
Matching a sample against a single stored template is called verification.



Searching a sample against many stored templates in the database is called identification.



Different biometric templates include following biometric systems:

Facial recognition	DNA
Voice recognition	Hand Geometry
Signature recognition	Finger Print
Retinal scanning	Iris recognition

All the above mentioned system is individually easy, accurate and somehow reliable, but short coming are due to high cost and security.
In spite of the fact, with previous problems disused in literature review section while moving, storing and extracting templates to and from cloud data bases, I think with use of the hybrid of Cognitive and Quantum cryptography approach we can resolve this security issues. Let us see the basic concepts of both approaches.

Cognitive Cryptography

Cognitive cryptography is used by splitting it and distributing the divided parts among selected groups of secret or concerned trustees for securing information. The process is concerned with concealing data by distributing secret parts or shadows with the use of cognitive techniques describing the personal information contained in each biometric template. It's very innovative and useful tool for securing data.
Pros: Used for data retrieval, data storage and data transfer in a secured manner.
Cons: Efficiency hinders because of level of security provided, computational speed, key size, cost and the algorithm.
Solution: Choosing the accurate bit for keys length in encryption and decryption data. Symmetric key algorithm can be used because of its high computational speed and low key size. [5]

Quantum cryptography

Quantum cryptography is used for secret communications. Its basic goals are the CIA triad – Confidentiality, Integrity, and Availability.
The Quantum Key Distribution is used for producing random key for communication between sender and a receiver. Key distribution assures no third party is involved.
Quantum key Protocols or algorithms

- BB84
- B92
- EPR.

These protocols communicate by interchanging qubits using quantum channel by applying sequence of key bits.
Cloud Computing service providers include big players like Google, Microsoft, Apple, Amazon and many other. The data transfer occurs at network level and storage level where allocation of resources and scheduling is provided by the cloud vendors. Also, help by preventing the breakthrough in malicious programs increasing cloud security. Every day hackers are trying to hack into some cloud even Apple and Dropbox being compromised, 10 cloud securities has become a new area of concern for researchers as well.

Proposed Algorithm

Hybrid of Cognitive and Quantum Cryptography

By Hybrid of cognitive and quantum cryptography advantages of both cryptography techniques are merged.
There by achieving our basic goal of safely encrypting, storing, decrypting and extracting the required template from data bases.
Consist of following steps:

1. **Sensors :** To detect biometric
2. **Signal processing :** Clear feature extraction
3. Cryptography approach:
4. **Quantum cryptography:** To generate a secret key
5. **Cognitive cryptography:** To Distribute template into sub templates
6. **Template Storage:** Store at different cloud databases or different parts of the same data base
7. Apply Cognitive Cryptography : To gather distributed parts of concerned template

8. **Merger:** Merge the distributed parts as one template
9. **Pattern Matching:** Closely matched to original template by using quantum secret key to avoid middle man attacks or data losses
10. **Decisions:** Is it true or false match.

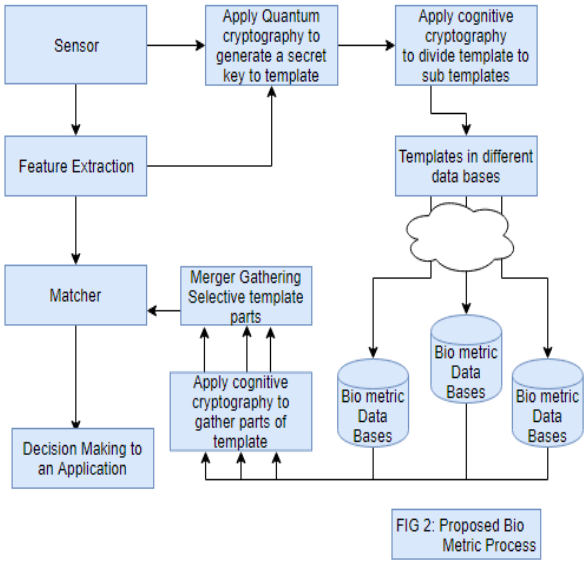


Fig. 2 The Proposed Bio metric Process

Problem

The major drawback I think in this proposed solution can be of larger space and storage.

The issue in qu bits and man in the middle attack is the second problem. There is a need to distribute, store and extract the biometric templates.

Qu bit problem is related to automatic flip flop in the number of bits, here 1 become 0 and 0 become 1.

Time consumption can also be increased but CIA goals are going to be fully accomplished.

Solution

The template is secure and safe to be retrieved later for usage.

However, for avoiding issues of larger space and storages, templates can be stored in DNA Storages inside the cloud.

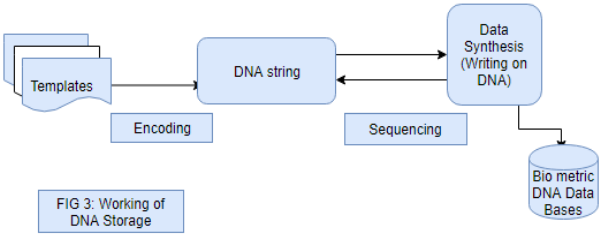


Fig. 3 Working of DNA storage inside the Cloud

DNA is durable and long lasting, three basic steps

Encoding: To convert template into 0 1 format

Storing: To store in DNA databases

Sequencing: To Retrieve stored template.

DNA uses long sequences of smaller molecules, called nucleotides – A for adenine, C for cytosine, T for thymine and G for guanine and creating sequences of 0s and 1s to store all type of data including picture, text, books, video and movies. Smaller chunks are made while storing data and on the retrieval, indicator is used to ensure the completeness. After the creation of DNA strand data is stored them in cold and blocks water and light to keep them dry. Time consuming and relatively slow even to take small information stored on a particular DNA, user have to go through all the data present on that DNA container. Two major reasons to use DNA Storages inside the cloud for safe and secure means of storing and retrieving the data

1. Traditional methods to store data might not be able to store the large amount of Big data
2. A single strand of DNA has quite a long life about millions of years to store that data safely.

Similarly, to avoid qu bits attack, lattice based cryptography can be used. Instead of bits the geometric objects will be used to send and store data. They are powerful and resistant to quantum attacks. Lattice based cryptography can be used to construct cryptographic primitives and boundaries Also help in hiding the data identity. For example, during auctions or data mining, during voting's and negotiations.

Table 2: Biometric main Problems and Solutions

Area	Problem	Solution
Biometric Templates	Storage	Cloud Data Bases
Cloud Data Bases	Insecure	Cryptography
Cryptography	Key distribution	Quantum Cryptography
Quantum Cryptography	Size, traffic, and delay of data Qu bits	Hybrid of QC algorithms and Pair Hand protocol or Lattice based Cryptography
Hybrid of QC algorithms and Pair Hand protocol	Heavy computation cost	Cognitive Cryptography
Cognitive Cryptography	Complex computing power	Hybrid of cognitive and quantum cryptography
Hybrid of cognitive and quantum cryptography	High storage required for storing distributed templates	Hybrid of QC+CC=DNA Storages
DNA Storages	Time Consuming Portability Expensive	Still in working how to overcome the limitations of DNA Storages

This review article critically analyzes the existing methods of storing biometric templates onto DNA to store massive amounts of data.

5. Conclusion

Short comings of DNA storage can be removed with some efficient algorithm like Genetic Algorithm for searching and scheduling requested data from the DNA data bases. Short comings of quantum cryptography can be reduced by using lattice based cryptography thus securing our templates more efficiently. As users are increasing day by day identification of a biometric template also requires more resources to compute, store, extract and scan records of a database to find best possible match.

This Review paper proposed a new cloud computing environment, which suggests future work by applying hybrid of Cognitive and Quantum key distribution while storing biometric templates in cloud DNA data base.

References

[1] Bala, Y., & Malik, A. (2018). Biometric Inspired Homomorphic Encryption Algorithm for Secured Cloud Computing. In Nature Inspired Computing (pp. 13-21). Springer, Singapore.

[2] Talreja, V., Ferrett, T., Valenti, M. C., & Ross, A. (2018, January). Biometrics-as-a-service: A framework to promote innovative biometric recognition in the cloud. In Consumer Electronics (ICCE), 2018 IEEE International Conference on(pp. 1-6). IEEE.

[3] Chand, K. S., & Rani, B. K. (2018). Biometric Authentication using SaaS in Cloud Computing.

[4] Ali, Z., Hossain, M. S., Muhammad, G., Ullah, I., Abachi, H., & Alamri, A. (2018). Edge-centric multimodal authentication system using encrypted biometric templates. Future Generation Computer Systems.

[5] Ogiela, M. R., & Ogiela, L.(2018) Cognitive cryptography techniques for intelligent information management. International Journal of Information Management, 40, 21-27.

[6] ArunPrakash, R., Jayasankar, T., & Vinothkumar, K. (2018). Biometric Encoding and Biometric Authentication (beba) Protocol for Secure Cloud in M-Commerce Environment. Appl. Math, 12(1), 255-263.

[7] Hahn, C., Shin, H., & Hur, J. (2017, July). Cloud-based biometrics processing for privacy-preserving identification. In Ubiquitous and Future Networks (ICUFN), 2017 Ninth International Conference on (pp. 595-600). IEEE.

[8] Zhang, C., Zhu, L., & Xu, C. (2017). PTBI: An efficient privacy-preserving biometric identification based on perturbed term in the cloud. Information Sciences, 409, 56-67.

[9] Kumari, S., Li, X., Wu, F., Das, A. K., Choo, K. K. R., & Shen, J. (2017). Design of a provably secure biometrics-based multi-cloud-server authentication scheme. Future Generation Computer Systems, 68, 320-330.

[10] Gawade, S., Bharti, A., Raj, A., & Madane, S. (2017). Biometric Authentication using Software as a Service in Cloud Computing. International Journal Of Engineering And Computer Science, 6(3).

[11] Tapase, P. G., Wazurkar, G. N., & Dandekar, D. R. (2018). Lossless Encryption Technique for Finger Biometric Images.

[12] Riaz, N., Riaz, A., & Khan, S. A. (2018). Biometric template security: an overview. Sensor Review, 38(1), 120-127.

[13] Živić, N., & Ruland, C. (2018, January). Cognition for enhanced biometrie authentication. In Information Networking (ICOIN), 2018 International Conference on (pp. 241-244). IEEE.

[14] Han, J., Liu, Y., Sun, X., & Chen, A. (2018). A self-adjusting quantum key renewal management scheme in classical network symmetric cryptography. The Journal of Supercomputing, 1-19.

[15] Ekert, A. (2018). Quantum cryptography: The power of independence. Nature Physics, 14(2), 114.

[16] Zhu, D., Li, X., Li, X., Wei, R., Wu, J., & Song, L. (2018). A Quantum Identity Authentication Protocol Based on Optical Transmission & Face Recognition. International Journal of Online Engineering (iJOE), 14(04), 58-69.

[17] Murugan, C. A., & KarthigaiKumar, P. (2018). Survey on Image Encryption Schemes, Bio cryptography and Efficient Encryption Algorithms. Mobile Networks and Applications, 1-6.

[18] Qiu, L., Cai, F., & Xu, G. (2018). Quantum digital signature for the access control of sensitive data in the big data era. Future Generation Computer Systems.

[19] Nautsch, A., Isadskiy, S., Kolberg, J., Gomez-Barrero, M., & Busch, C. (2018). Homomorphic Encryption for Speaker Recognition: Protection of Biometric Templates and Vendor Model Parameters. arXiv preprint arXiv:1803.03559.

[20] Sarier, N. D. (2018). Multimodal biometric Identity Based Encryption. Future Generation Computer Systems, 80, 112-125.

[21] Droandi, G., Barni, M., Lazzeretti, R., & Pignata, T. (2018). SEMBA: SEcure multi-biometric authentication. arXiv preprint arXiv:1803.10758.

[22] Sarkar, A., Singh, B. K., & Bhaumik, U. (2018). Cryptographic Key Generation Scheme from Cancellable Biometrics. In Progress in Computing, Analytics and Networking (pp. 265-272). Springer, Singapore.

[23] Hesketh, E. E., Sayir, J., & Goldman, N. (2018). Improving communication for interdisciplinary teams working on storage of digital information in DNA. F1000Research, 7.

[24] Lear, G., Dickie, I., Banks, J., Boyer, S., Buckley, H. L., Buckley, T. R., ... & Kamke, J. (2018). Methods for the extraction, storage, amplification and sequencing of DNA from environmental samples. New Zealand Journal of Ecology, 42(1), 10-50A.

[25] Pal, R., Anand, T., & Dubey, S. K. (2018). Analytical and Perspective Approach of Big Data in Cloud Computing. In Big Data Analytics (pp. 233-239). Springer, Singapore.

[26] Shabani, M., Vears, D., & Borry, P. (2018). Raw Genomic Data: Storage, Access, and Sharing. Trends in Genetics, 34(1), 8-10.

[27] Li, S., Liu, J. K., Zhao, G., & Wang, J. (2018). CADS: CRISPR/Cas12a-Assisted DNA Steganography for Securing the Storage and Transfer of DNA-encoded Information. ACS synthetic biology.

[28] Lear, G., Dickie, I., Banks, J., Boyer, S., Buckley, H. L., Buckley, T. R., ... & Kamke, J. (2018). Methods for the extraction, storage, amplification and sequencing of DNA from environmental samples. New Zealand Journal of Ecology, 42(1), 10-50A.
[29] Trivedi, D., Thanki, R., & Kothari, A. (2014). Biometric Template Feature Extraction and Matching Using ISEF Edge Detection and Contouring Based Algorithm. International Journal of Engineering Research and General Science, 2(4).
[30] Murugan, C. A., & KarthigaiKumar, P. (2018). Survey on Image Encryption Schemes, Bio cryptography and Efficient Encryption Algorithms. Mobile Networks and Applications, 1-6.

Mehreen Ansar received the B.S. degrees in Computer Engineering from Bahauddin Zikariya University, Multan in 2012 and doing Master degree from Riphah International University, Faisalabad 2017 to 2019, respectively. Her BS project was based on Server Clustering, done with Windows Server 2008 and Linux. She is working as a web developer since 2012. Her domain lies in networking and security. Her main areas of research are Server Clustering; Cryptography, Cryptography protocols in Cloud Computing, Biometrics, and Cloud Migration.

Mubeen Fatima was born in Faisalabad; Punjab, Pakistan in 1993.She received the BS degree in Software Engineering from National University of Sciences and Technology (NUST), Islamabad in 2015. She is currently student of MS in Information Security from National University of Sciences and technology (NUST), Islamabad. The MS degree will be complete in 2019. She is working as a SAP Trainer in SEIMENS, Islamabad. Her domain lies in networking and security. Her main areas of research are Cryptography, IOT, Machine Learning and Artificial Intelligence.