International Journal of Engineering Innovation & Research
Volume 9, Issue 6, ISSN: 2277 – 5668

Secure Cloud Simulation Using Hybrid Algorithm

B. Reena [1*], P. Divya [2] and I. Jasmine Selvakumari Jeya [3]
[1, 2] Assistant Professor, Department of Computer Science and Engineering, Hindusthan College of Engineering and Technology, India.
[3]Associate Professor, Department of Computer Science and Engineering, Hindusthan College of Engineering and Technology, India.
*Corresponding author email id: breena.cse@hindusthan.net

Date of publication (dd/mm/yyyy): 03/12/2020

***Abstract* – At present, data security and privacy has been regarded as one of the biggest concerns in cloud computing. Data stored remotely is vulnerable and susceptible to threats. Due to this, users do not trust their data over the cloud. Cloud consumers want an assurance that they can access their data wherever they want without anyone else's manipulation. Moreover, authentication of users over the cloud is another important factor to consider. After conducting surveys and studying various research papers it is found that the major security concerns of cloud computing includes Data leakage, Distributed Denial of Service (DDOS). The data security can be improvised by implementing various symmetric key algorithms so that data on the server is stored in such a manner that even if a person can access the data, they can't view the original data, as it needs to be decrypted. Including storage security, authorized access of users also helps in avoiding DDOS as only genuine users will have access to the cloud. A hybrid model, a mixture between elliptical curve cryptography and symmetric key algorithm in which ECC is used for user verification and to keep the private data secure while AES algorithm is used to allow the user to store and access their data securely in the cloud by encrypting the data on the client side and decrypting the data after downloading from the cloud. Since the private key is owned by the user of the data, none can decrypt the data, even if hackers get their hands on the data. Moreover, the user will securely authenticate themselves by using various input parameters at the time of login to the cloud server. The whole prototype of the proposed solution would benefit by enabling a proper access mechanism to avoid unauthorized access to the information system and secure storage to allow access of data.**

***Keywords* – Authentication, Data Leakage, Distributed Denial of Service (DDOS), Elliptical Curve Cryptography and Symmetric Key Algorithm.**

I. INTRODUCTION

Cloud Computing is the form of computing where resources are provided as services on the internet. There are three types of services in Cloud Computing which are used for the deployment of the application on the cloud. Data on the cloud will become more scalable, Reliable and Secure. The big names in Cloud Computing are AWS, Google, Microsoft and IBM. Cloud Computing is based on five attributes such as Shared Resources, Scalability, Pay to use, Elasticity and Self Provisioning of Resource. Most enterprises are shifting their applications on to the cloud owing to its speed of implementation and deployment, improved customer experience, scalability, and cost control. The services in Cloud Computing are SaaS, PaaS, laaS amongst which we are using PaaS and laaS service for deployment of Application on the Cloud in our Project. This service exhibits five essential characteristics such As Rapid Elasticity, Resource Pooling, on demand Self-service, Broad Network Areas. Data is being transmitted between two clouds so in order to secure the data most of the systems use the combination of techniques, including: Encryption, Authentication, Separation of duties.

These security parameters are achieved due to which the performance increases and therefore security is obtained to a higher extent. Data security and privacy risks have become the primary concern for people to shift to cloud computing. Cloud Computing is mainly used for improving data handling capability where the services

and the resources will be delivered continuously when and where required, due to which the Cloud computing is in great demand. However there still exist many problems in cloud computing today, as a recent survey shows that data security and privacy risks have become the primary concern for people to shift to cloud computing. Cloud is the free space where the application is being saved securely and the services are being provided continuously when and where required.

1.1. *Motivation*

Need of data security is an essential issue in the domain of computing traditionally. There are various algorithms that are developed in order to improve the security of data, but they have their own issues. Nowadays, the traditional algorithms are not much suitable for providing security over the untrusted communications and data exchange.

ECC is more and more considered as an attractive public-key cryptosystem for mobile/wireless environments. One of the other recent public key cryptosystems is Elliptic Curves Cryptography used for security. In recent times, the majority of e-commerce applications are designed using asymmetric cryptography to assure the authentication of the concerned parties. Compared to traditional public-key cryptosystems like RSA or Diffie-Hellman, ECC proposes equivalent security with smaller key sizes; these result in faster calculation, lower power expenditure, as well as memory and bandwidth savings. ECC is particularly useful for mobile devices, which are typically particular in terms of their CPU, power and network connectivity. Therefore, a new encryption standard is required that can fulfill the current need of security meanwhile that is extendable according to the need. The proposed work includes the development of new hybrid algorithms using ECC, ECDH and AES algorithms along with encryption techniques.

II. RELATED WORK

Qin Liu, Guojun Wang, and Jie Wu analyzed that the principle concept used here for the encryption process is hierarchical identity based encryption algorithm, which takes the number, as well as the public keys of the recipients as input [1]. This input is presented to the user at the upper level. The upper level user then encrypts the file only once and stores only one copy in the cloud and then sends the encrypted file to all the lower level recipients and this encrypted file is then decrypted by each lower level user with the help of their own private key.

Uma Somani, Kanika Lakhani, Manish Mundra examined by emphasizing more on common problems in cloud computing such as security and data, files system, backups, network traffic and host security [2]. To overcome these issues, digital signatures with RSA algorithm need to be used. The sender receives the documents from the cloud then it is broken into a number of lines with the help of hashing algorithm and these lines are called Message Digest. After this, the sender encrypts Message digest with his private keys and this results in the formation of digital signature. Now, the sender encrypts the digitally signed sign with the receiver's public key and finally the receiver decrypts it with his private key and the sender's public key, for verification, all while using RSA algorithm.

Ashutosh Kumar Dubey, Animesh Kumar Dube, Mayank Namdev, Shiv Shakti Shrivastava focused on the increased need of connectivity and the amount of data which requires large resources with dynamic load and access balancing [3]. This results in the use of cloud computing but with some security concerns regarding the

cloud computing environment. Thus, a new cloud computing environment which is controlled both by the client, and by the cloud environment administrator. For this purpose, RSA and MD5 algorithms are deployed. When the cloud user uploads data onto the cloud, the data uploaded is encrypted using RSA algorithm and the cloud admin can decrypt using their own private key. For updating the data on the cloud, the admin requests the user for a source key. The cloud user then sends a secure key with a message digest tag for updating the data. If any outsider performs a change in the key, the tag bit is also changed, indicating that the key is insecure.

Arthur Resumed, Henry C.H. Chen, Yang Tang, Patrick P.C. Lee, laid emphasis on cloud storage that enables individuals to outsource the storage of data backups to remote cloud providers at a low cost [4]. We present Fade Version, a secure cloud backup system that serves as a security layer on top of today's existing cloud storage services. It also follows the standard version control backup design that eliminates storage of redundant data across different backup versions. Above all, the Fade version also applies cryptographic protection to the data backup as well.

Cong Wang, Kui Ren,Wenjing Lou, Jin Liexplained that in order to facilitate rapid deployment of cloud data storage service and regain security assurances with outsourced data dependability, efficient methods that enable on-demand data correctness verification on behalf of cloud data owners have to be designed and thus proposed that publicly auditable cloud data storage is able to help this nascent cloud economy become fully established [5]. With public auditability, a trusted entity with expertise and capabilities data owners do not possess can be delegated as an external audit party to assess the risk of outsourced data when needed.

Adam Gordon understood that despite their need or desire to migrate their high-value data into cloud workloads, many enterprises hesitate to do so because of the risks associated with operation of the cloud models hosting this data [6]. In addition, a general lack of knowledge and understanding of cloud computing is keeping many organizations from adopting and using cloud platforms and services overall. As a means to examine this trend, the author considers the role of the cloud security professional in a hybrid cloud environment. He explores the need for training and certification options and identifies key areas of focus for the cloud computing professional.

Ahmed Albugmi, Madini O. Alassafi, Robert Walters, Gary Wills discussed the security of data in cloud computing [7]. It is a study of data in the cloud and aspects related to it concerning security and went into detail of data protection methods and approaches used throughout the world to ensure maximum data protection by reducing risks and threats. Availability of data in the cloud is beneficial for many applications but it poses several risks by exposing data to applications which might already have security loopholes in them. Likewise, use of virtualization for cloud computing might risk data when a guest OS is run over a hypervisor without knowing the reliability of the guest OS which might also have security loopholes in it. The paper will also provide an insight on data security aspects for Data-in-Transit and Data-at-Rest. The study is based on all the levels of SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service).

Valluru, D., I. Jasmine Selvakumari Jeya, presented lung cancer detection using Optimal Support vector machine, and the same was stored in Cloud for better accessibility [12]. The main reason behind selecting optimal features was fine-tuning the SVM for better prediction. The feature selection in the SVM classification was controlled by the Hybridized algorithm namely modified grey wolf optimization algorithm combined with genetic algorithm (GWO-GA). The results shows better feature selection and classification.

Cloud computing providers expose a set of software user interfaces (UIs) or application programming interfaces (APIs) that customers use to manage and interact with cloud services. Provisioning, management, orchestration and monitoring are all performed with these interfaces. The security and availability of general cloud services is dependent on the security of these basic APIs. APIs and UIs are generally the most exposed part of a system, perhaps the only asset with an IP address available outside the trusted organizational boundary. These assets will be the target of heavy attack, and adequate controls protecting them from the Internet are the first line of defense and detection.

Denial-of-service (DoS) attacks are attacks meant to prevent users of a service from being able to access their data or their applications. By forcing the targeted cloud service to consume inordinate amounts of finite system resources such as processor power, memory, disk space or network bandwidth, the attacker—or attackers, as is the case in distributed denial-of-service (DDoS) attacks—causes an intolerable system slowdown and leaves all legitimate service users confused and angry as to why the service is not responding.

III. PROPOSED SYSTEM

Need of data security is an essential issue in the domain of computing traditionally. There are various algorithms that are developed in order to improve the security of data, but they have their own issues. Nowadays, the traditional algorithms are not much suitable for providing security over the untrusted communications and data exchange.

ECC is more and more considered as an attractive public-key cryptosystem for mobile/wireless environments. One of the other recent public key cryptosystems is Elliptic Curves Cryptography used for security. In recent times, the majority of e-commerce applications are designed using asymmetric cryptography to assure the authentication of the concerned parties. Compared to traditional public-key cryptosystems like RSA or Diffie-Hellman, ECC proposes equivalent security with smaller key sizes; these result in faster calculation, lower power expenditure, as well as memory and bandwidth savings. ECC is particularly useful for mobile devices, which are typically particular in terms of their CPU, power and network connectivity.

Therefore, a new encryption standard is required that can fulfill the current need of security meanwhile that is extendable according to the need. The proposed work includes the development of new hybrid algorithms using ECC, ECDH and AES algorithms along with encryption techniques.

A hybrid model is proposed which is a mixture of elliptical curve cryptography and symmetric key algorithm. ECC is used to achieve the process of user's verification and to keep the private data secure. AES algorithm is used which allows the user to store and access their data securely to the cloud by encrypting the data in the client side and decrypting the data after downloading from the cloud. Since the private key is owned by the user of the data, no one can decrypt the data, even though hackers can get the data through other means.

Moreover, the user will securely authenticate themselves by using different input parameters at the time of login to the cloud server. This scheme can make users confident about the security of the data stored in the cloud. Here, ECC and ECDH algorithms are applied, which provide the same level of security as compared to other public key cryptosystems, with less key size and also strengthens the security of the algorithm. The whole prototype of the proposed solution would benefit by enabling a proper access mechanism to avoid unauthorized access to the information system and a secure storage to allow access of data over the cloud network.

3.1. *Implementation Outline*

Initially the user is taken to the landing page of the web application which lets the user know about the application and lets the user choose between first time registration and login features. Along with this, the page contains tabs for the download and uploads section. The Registration Page of the application is displayed when the user is using the application for the first time or does not possess a user account. It takes the user's details as input to store user's information and validate the user before giving access to the app data. It first checks for all possible errors in the credentials on the client side itself using regular expressions and pattern matching. Later, if the data passes all the test cases, it is sent to the server side to validate and store the details in the database to create a working profile of the user. Using the ECC algorithm, public key and private key both are generated. Here, the sender encrypts the data and the receiver decrypts the data by using their own private key. The form here takes registration number along with secret key for successful key exchange. Upon automatic ECDH key agreement, OTP (one time password) is sent to the email address given by the user on stage one of the registration. The app takes OTP as input and after proper validation of both the fields, it passes the control to the next stage of new user registration and on successful validation, the application generates a unique User ID. The user is requested to save this ID as, once the registration is done, the user will be using just the User ID generated here and the secret key entered earlier to use all the features and perform validation further in the application. The new user registration completes here and now the user can easily login to access his profile and use all the features of the application. When the user is able to successfully login into the app for the first time, the user is taken to the My Account section where they are shown the current details of his account stored in the database and given an opportunity to update any field if required and click on the submit button to save. The user can upload a file in the cloud and to encrypt and ensure security, they would hit the encryption tab. The encryption key is then required which is actually the secret key entered at the time of registration also. After that, the file to be uploaded from the local system on which the application is running is selected. Now after the encryption and uploading of the file is done, the user can go to the decryption section, enter the respective AES key that was generated and given to the user, and select the file to download. After this, the chosen file is decrypted and ready for download. The downloading would start as soon as the user hits the download button.

3.2. *Architecture Diagram*

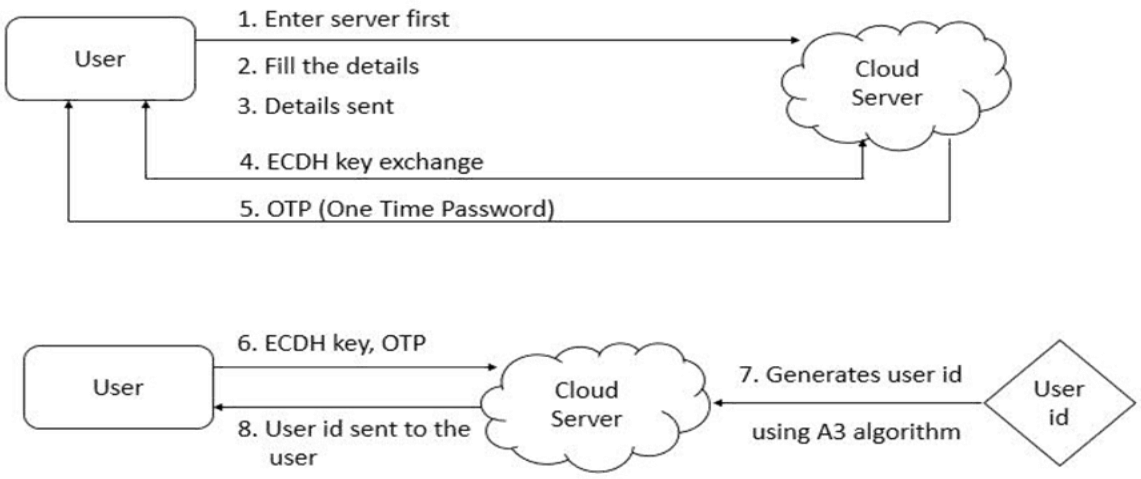


Fig. 3.1. Overall architecture with component description and dependency details.

IV. WORKING MODEL

Each requirement maps to a higher-level function that transforms the given set of input data into output data. The functional requirements can be identified as the modules involved. These modules perform separate functions based on the given input and return output data for the next level. Different types of functional requirements possessed by the system are:

1. Introduction Module.
2. Registration Module.
3. Key Exchange Module.
4. ID Generation Module.
5. Login Module.

Module 1: Introduction Module

Purpose – A brief introduction. It is invented to be engaging and communicate the theme of the cloud application to the user.

Inputs – No input is necessary.

Outputs – Immediately load the Main Menu Screen (Registration Screen)

This is the landing page of the web application – the very first page which is visible when the app is launched in the browser of the user's system. This page lets the user know about the application and let the user choose between first time registration and login features. Along with this, the page contains tabs for the download and upload section. It contains, app logo, tag line and makes the user aware about the goal of the application for a short period of time and enhances aesthetic value.

Module 2: Registration Module

Purpose – The central point after connection establishment. The menu responds to user clicks and details are sent to the server.

Inputs – Username, Mobile Number, Email, DOB fields are displayed, submit button. Outputs – Control is passed to the key exchange page with a random registration created.

This is the Registration Page of the application which is displayed when the user is using the application for the first time or does not possess a user account. The form here takes the user's full name, email address, mobile number, DOB and gender as input to store user's information and validate the user before giving access to the app data. It first checks for all possible errors in the credentials on the client side itself using regular expressions and pattern matching. Later, if the data passes all the test cases, it is sent to the server side to validate and store the details in the database to create a working profile of the user.

Module 3: Key Exchange Module

Purpose – For ECCDH equivalent key exchange. Inputs – Secret Private Key for exchange.

Outputs – ECDH Key is generated and OTP sent to mail ID.

This is the Key Exchange page of the application. Using the ECC algorithm, public key and private key both are generated. Here Sender will be used to encrypt the data and receiver i.e. B is used to decrypt the data by using its own private key. The form here takes, registration number along with secret key for successful key exchange.

Module 4: ID Generation Module

Purpose – For user ID generation. Generation of user ID. Accessing the cloud storage. Fresh OTP sent to email ID.

Inputs – OTP from email ID in the text field. User ID and OTP Request.

Outputs – Random user ID is generated. OTP verification and redirecting to the user account.

This is the 3rd stage of Registration process itself. Here ECDH key agreement has been automatically generated successfully and OTP (one time password) is sent to the email address given by the user on stage one of the registration. The app takes OTP as input and after proper validation of both the fields, it passes the control to the next stage of new user registration.

On successful validation, the application generates a unique User ID. The user is requested to save this ID as, once the registration is done, the user will be using just the User ID generated here and the secret key entered earlier to use all the features and perform validation further in the application. The new user registration completes here and now the user can easily login to access his profile and use all the features of the application.

Module 5: Login Module

Purpose – To check credentials of the user and log in if they are correct and grant the access to their account.

Inputs – User ID and the OTP sent to the user's email ID.

Outputs – Immediately load the Profile Screen if the credentials match.

This is the Login page of the application which is loaded when the user clicks on the login tab button. The page consists of a simple form which inputs the User ID of the user generated during the registration process and the OTP which is immediately sent to the user's email address as soon as he clicks on 'Request for OTP' button in the form. Later, both the values in the fields are validated over the server with the values in the database and if successful the user is taken to the next page that is Dashboard of the application, else error is generated. Here a confirmation message is shown to verify that the OTP is successfully delivered to the registered email ID of the user.

When the user is able to successfully login into the app for the first time, the user is taken to the My Account section where he is shown the current details of his account stored in the database and is given an opportunity to update any field if required and click on the submit button to save. The dashboard page serves as a navigating page as from here the user can go-to encryption, decryption download and upload sections and can log out from the app if the work is done.

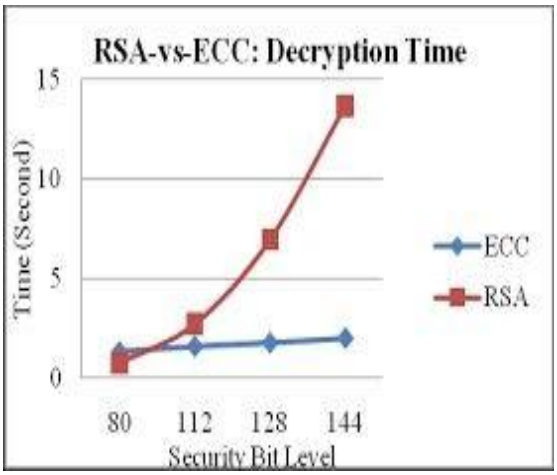
If the user wishes to upload a file in the cloud application and encrypt it to ensure security, he would hit the encryption tab. Next he is asked to enter the Encryption key which is actually the same secret key entered at the time of registration also. After that, he is asked to select the file to be uploaded from his local system on which

the application is running. Lastly, click on submit to process the encryption and saving of the file.In the final dashboard of the user's account, the user can go to the decryption section, enter the respective AES key that was generated and given to the user, and select the file to download. After this, the chosen file is decrypted and ready for download. The downloading would start as soon as the user hits the download button.

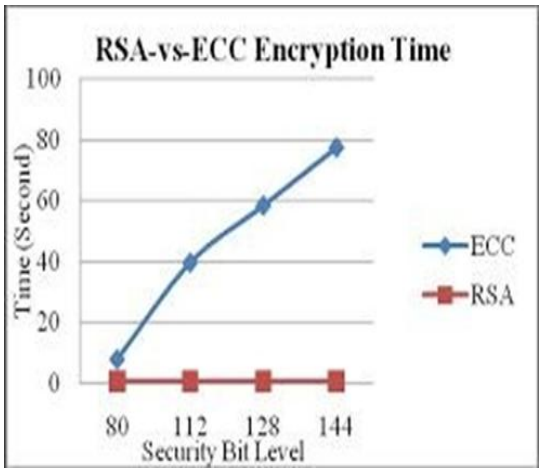
V. Performance Analysis

5.1. *Comparative Analysis of RSA and ECC*

On a test done on three sample data inputs each of 8,64 and 256 bits respectively, the efficiency of ECC over RSA can be understood. These experiments were done on MATLAB R2008a on Intel Pentium dual-core processor (1.60 GHz, 533 MHz, 1 MB L2 cache) with 2GB DDR2 RAM. Based on experimentation, it is observed that RSA is very efficient and quick in encryption [Graph 2.] but slow in decryption [Graph 1] while ECC is slow in encryption but very efficient in decryption. Overall ECC is more efficient and secure than RSA.



Graph 5.1.



Graph 5.2.

Security of the message is paramount during its transmission from one user to another user or system. While symmetric-key cryptography is very good in providing security to the message, it suffers from key distribution and management problems. To mitigate the key distribution and management problems and to ensure confidentiality, and integrity of a message, asymmetric-key cryptography was invented by Diffie-Hellman. The experimentation was conducted for finding time lapse during encryption, decryption by RSA and ECC on three sample input data of 8 bits, 64 bits, 256 bits with random keys based on NIST recommendation. Based on experimentation, it can be concluded that ECC outperforms RSA regarding operational efficiency and security with lesser parameters.ECC is particularly most suitable for devices with limited resources, both storage and processing, making it highly viable in the current cloud sector.

VI. Conclusion

This paper simulates a model that is already quite common for consumer apps like email and photo sharing, and for certain business applications. But in this paper, we present a way to secure the data using different security techniques and efficient encryption algorithms to secure the file along with its location from the users that stores and retrieves it. As with the Internet, on-demand applications have grown so ubiquitous that almost every business user interacts with at least one, whether it's an email service, a Web conferencing application, or

a file hosting system.

The data is stored at multiple places over the information space (over the Internet). It sounds similar to file hosting websites which stores the data that is being uploaded by different users and can be retrieved using proper authentication. The only difference is that the system for which project is targeted is an application based system like which will run on the client's own system. This application will allow users to upload files of different formats with security features including Encryption, secure OTP verification, uploading and downloading over the cloud securely.

This prototype works using a mixture of elliptical curve cryptography and symmetric key algorithm. ECC is used to achieve the process of user's verification and to keep the private data secure. AES algorithm is used to allow the user to store and access their data securely to the cloud by encrypting the data on the client side and decrypting the data after downloading from the cloud. Since the private key is owned only by the user of the data, no one can decrypt the data, even though the hacker can get the data through some approaches.

The uploaded files can be accessed from anywhere using the application which is provided. We believe this system serves as a foundation for future work in integrating and securing information sources across the World Wide Web.

REFERENCES

[1] Qin Liu, Guojun Wang, and Jie Wu "Efficient Sharing of Secure Cloud Storage Services" 2010. 10th IEEE International Conference on Computer and Information Technology (CIT - 2010).
[2] Uma Somani, Kanika Lakhani, Manish Mundra "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing" 2010 IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).
[3] Ashutosh Kumar Dubey 1, Animesh Kumar Dubey 2, Mayank Namdev3, Shiv Shakti Shrivastava "Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment "in 2011.
[4] Xiang Tana, Bo Aib "The Issues of Cloud Computing Security in High-speed Railway "in 2011.
[5] Arthur Rahumed, Henry C.H. Chen, Yang Tang, Patrick P.C. Lee, and John C.S. Lui "A Secure Cloud Backup System with Assured Deleti-
-on and Version Control" 2011 International Conference on Parallel Processing Workshops.
[6] Eman M. Mohamed and Sherif EL-Etriby "Randomness Testing of Modem Encryption Techniques in Cloud Environment" in 2008.
[7] C. Wang, K. Ren, W. Lou and J. Li, "Toward publicly auditable secure cloud data storage services,", July-August 2010.
[8] A. Gordon, "The Hybrid Cloud Security Professional," in IEEE Cloud Computing, Jan.-Feb. 2016.
[9] A. Albugmi, M.O. Alassafi, R. Walters and G. Wills, "Data security in cloud computing," 2016 Fifth International Conference on Future Generation Communication Technologies (FGCT), Luton, 2016.
[10] Zhengbing Hu, Sergiy Gnatyuk, Oksana Koval, Viktor Gnatyuk and Serhii Bondarovets," Anomaly Detection System in Secure Cloud Computing Environment", I.J. Computer Network and Information Security, 2017.
[11] Nagesh M. Wankhade, Kiran A. Sahare, Prof. Vaishali G. Bhujade ," Secure Cloud Simulation Using Triple Des", International Journal of Research in Advent Technology, January 2014.
[12] Valluru, D., I. Jasmine Selvakumara Jeya, IoT with cloud based lung cancer diagnosis model using optimal support vector machine, Health Care Management Science (2019).
[13] Lo'ai Tawalbeh, Nour S. Darwazeh, Raad S. Al-Qassas, Fahd Al Dosaria," A Secure Cloud Computing Model based on Data Classification", Procedia Computer Science, 2015.
[14] I Jasmine Selvakumari Jeya & J Suganthi, Survey of Secure Multimedia Database using Public Key Cryptography Method and Optimization Techniques, International Journal of Engineering Innovations and Research, 2012.
[15] Jasmine Selvakumari Jeya I, M. Uma Priya & M. Revathi, "Survey of Security Issues in Various Database using Digital Watermarking Techniques", International Journal of Engineering Innovation & Research, 2018.
[16] Brindha T, Shaji RS, Rajesh GP." A Survey on the Architectures of Data Security in Cloud Storage Infrastructure" International Journal of Engineering &Technology, 2013.
[17] Mahmood, Z." Data location and security issues in cloud computing", IEEE International Conference on Emerging Intelligent Data and Web Technologies, 2011.

AUTHOR'S PROFILE

First Author
B. Reena, currently working as Assistant Professor in the Department of Computer Science and Engineering at Hindusthan College of Engineering and Technology, Coimbatore. She has completed bachelor degree in Information Technology from VLB Janakiammal College of Engineering and Technology, Coimbatore in 2003, M.E degree in Computer Science and Engineering from Dr. Mahalingam College of Engineering and Technology, Pollachi in the year 2008. She has more than 11 years of experience in teaching. The area of interest includes Data Mining, Cloud Computing, Big Data, Data Science, Internet of Things, etc.

Second Author

P. Divya, currently working as an Assistant Professor in Department of Computer Science and Engineering, Hindusthan College of Engineering and Technology, Coimbatore. She has more than 9 years of teaching. She has completed bachelor degree in B. Tech, Information Technology in Karpagam College of Engineering, Coimbatore in 2009, M.E. degree in Computer Science and Engineering from Karpagam University, Coimbatore in 2011. She has presented four papers in international conference. The area of interest includes Java Programming, Python Programming, C and C++ Programming, Database Management Systems, Big Data Analytics, etc.

Third Author

Dr. I. Jasmine Selvakumari Jeya, currently working as an Associate Professor in Department of Computer Science and Engineering, Hindusthan College of Engineering and Technology, Coimbatore. She has more than 18 years of teaching and research experience. She has completed bachelor degree in Computer Science and Engineering from C.S.I. Institute of Technology, Nagercoil in 2001, M.E degree in Computer Science and Engineering from Karunya University, Coimbatore in 2007 and her PhD degree in Medical Image Database Security under faculty of Information and Communication Engineering in the year 2016 at Anna University. She has published more than 18 research papers in In--ternational Journals with good impact factor, 42 International and National Conferences and two books. She has received active participation award for Woman member and Longest Continuous Student Branch Coordinator award from the Computer Society of India (CSI). The area of interest includes Medical Image Database Security, Information Security, Image Processing, Data Mining, Cloud Computing, Big Data etc. She is a life member of Institution of Engineers and Computer Society of India. She is a recognized supervisor in Anna University and guiding PhD scholars under her supervision.