IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ENHANCING SECURITY USING ECC IN CLOUD STORAGE

[1]Tejaswi Kumbhar, [1]Rahul Gaikwad, [2]Srivaramangai R

[1]Student, [1]Student, [2]Supervisor

[1]Department of Information Technology,

[1]University of Mumbai, Mumbai, India

Abstract: Due to its smaller key sizes and quicker computations when compared to conventional public key cryptography algorithms, ECC is a subset of public key cryptography that has grown in popularity. The paper investigates the foundations of ECC. The article also covers several popular ECC algorithms. With the help of the Elliptic Curve Cryptography algorithm, this work aims to provide security services like confidentiality for cloud services. Because of its benefits in terms of smaller key sizes, less CPU time, and less memory usage, it should be used for data encryption rather than the well-known and widely used RSA algorithm. This survey paper provides an overview of the key concepts and applications of (ECC).

Index Terms - **Cryptography, Bandwidth, Decryption algorithm, Key Generation, Signature Verification**.

I. INTRODUCTION

Data storage in the cloud has grown in popularity among individuals and businesses, but security issues remain a big problem. Using (ECC) is one way to increase cloud storage security. Public key cryptography called ECC is based on the algebraic design of elliptic curves. Compared to conventional public key cryptography algorithms, it has several benefits, including faster computations and smaller key sizes. ECC is a good fit for cloud storage because of these benefits because efficiency and security are both important.

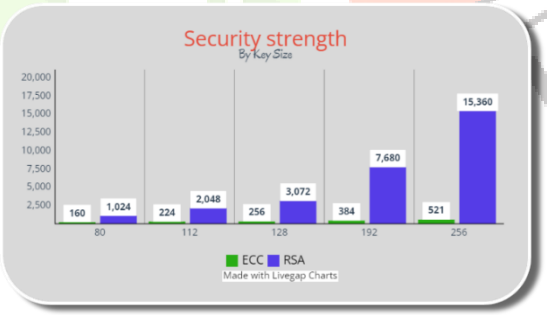

Fig.1: - Security strength between ECC& RSA

1.1 Security issues

Below are some of the common causes, found for the need for cryptography and data security:

1.1.1 Data Breach

It has a hap that requires the illegal or illegal viewing access or recoupment of data which can be handed over by an individual play or service it has a kind of security breach that is particularly composed to steal and or advertising data to a slackened or illegal place a data breach has also feted as a data slip or data leak a data breach happens when an unauthorized hacker or bushwhacker reaches a secure database or depository data breaches have generally handed towards applicable or digital data and hourly delivered across the internet or a network connection a data breach may affect data loss which may be linked with fiscal private and health information a hacker may also work removed data to portray himself for securing access to a redundant secure position for illustration a hackers data breach of a network directors login credentials may affect in the approachability of the entire network.

1.1.2 Kidnapping of accounts

It has a system for hackers to try to take the private dispatch account machine account or some other description connected with a computing machine or service it has a kind of identity theft in which the hacker works the commandeered account data to bring out the vicious or illegal movement the completion and perpetration of the pall in several diligence have started a new set of

problems in account kidnapping bushwhackers can manage your or your worker's login information to ever access sensitive data stored on the pall also bushwhackers can falsify and manipulate data through the commandeered credentials.

1.1.3 Trouble from the inside

The attacks on any organizational coffers and services may be initiated by the different type of interferers primarily including interposers interferers as well as stranger interferers the pitfalls of gaining authorized access by sanctioned person s associated with the association is known as bigwig pitfalls the bigwigs pitfalls are primarily executed by the workers of the association to pierce the nonpublic information of the association through their authentication and authorized rights the identification and running of similar pitfalls is a major challenge for icing the effective security of the system the low probability of passing similar pitfalls increases the complexity of the handling similar pitfalls occasionally these types of vicious attacks are happens unintentionally so along with the security policy the procurement of system also becomes a major concern for these type of systems the study of colorful literature and several practices espoused by association highlights that bigwig pitfalls are generally carried out with the intent of misusing the information having suspicious and wrong station of the bushwhacker for the associations the popular diving ways for handling similar pitfalls are designing secured programs to land the intellectual coffers establishing business hookups prioritizing enterprise controlling access and enforcing effective technologies for secured system.

1.1.4 Malware injection

The bushwhackers may essay to pierce the sensitive and nonpublic information through the vicious software injections these software injections are the specialized scripts or law bedded into the associations pall services, the pall services considers processes generated by these software injections as valid cases and allows them to execute with proper authentication and needed boons the cloud server permits these canons to execute software as a service SaaS on the pall waiters similar prosecution of vicious pitfalls makes the identification and handing of these pitfalls not only a relatively grueling task but also increases the failing probability of the system the prosecution of similar vicious injection canons forces the pall waiters to bear abnormally on regular base and during this abnormal prosecution of pall waiters the bushwhackers may exploits the security loopholes of the system to gain unauthorized access of the nonpublic and sensitive information the bushwhackers may perform colorful attacking ways primarily including wiretapping compromising the integrity of sensitive information and attempt to stealing the precious data the study of colorful literature specifically on security pitfalls on cloud computing illustrates that pitfalls grounded on of malware injections has come a serious and major concern for the secured data processing and communication on pall computing and has come a primary choice of experimenters in the sphere of pall computing surroundings.

1.1.5 Abuse of cloud services

The vituperative relinquishment of pall services has one of the major cloud calculating pitfalls. The increase of pall services has produced it doable for both small and enterprise- position businesses to host large figures of data painlessly but the palls unique storehouse volume has also handed both hackers and authorized druggies the to comfortably host and spread malware illegal software and other digital coffers in many cases this system affects both the pall service provider and its customer for illustration furnished druggies can incontinently or diagonally ameliorate the security pitfalls and as a conclusion worm upon the terms of use handed by the service provider.

1.1.6 Data loss

The bushwhackers attempts to gain unauthorized access of sensitive data by launching variety of attacks similar attacks may also induce large quantum of data loss during data communication and recycling the needed data on miscellaneous pall waiters the rigorous attempts of attacks may have different types of impact on the pall systems these can be in form of data corruption attainability of sensitive data omission of nonpublic and sensitive data unanticipated changes by unauthorized druggies loose software or services performing services vital to the system data loss may be not only due to vicious attacks on the pall services can be but it may also be due to natural disaster or a data wipe by the service provider the data loss may be veritably pivotal form any association and the situation may come more adverse if the concerned association doesn't have a recovery plan one the popular and major data losses is the case of data loss happed at amazon the data loss at amazon association is an illustration of an association that suffered data loss and accordingly forced to permanently cancel the large quantum of their own vicious guests data in 2011. Another illustration of data loss is the case of data loss happed at Google another association that lost its data due to the frequent disturbances of the power grid the long list of similar exemplifications reveals that securing organizational data isn't only limited to the security of the digital data but also it must be accompanied with suitable back over procedures as well as the proper security of to physical storehouse locales proper monitoring of physical access and handling the probable physical disasters.

1.1.7 Denial of service attacks

It has a kind of attack wherever the interferers hackers bid to limit genuine druggies from reaching the service in this kind of attack the bushwhacker naturally gives spare dispatches requesting the network or server to validate requests that should wrong answer locales the network or server won't be able to gain the recovery address of the bushwhacker when transmitting the authentication authorization producing the garcon to stay before terminating the connection the bushwhacker transmits also authentication dispatches with invalid return locales at the ending kind of the connection with the garcon as an outgrowth of this operation the system of authentication and garcon stay will be admitted over which would hold the network or server busy for a longer period unlike different kinds of cyberattacks which have generally thrust to make a long- term base and commandeer sensitive data service charges don't strive to transgress your security boundary rather a certain kind of bushwhackers bid to capture the design of the stoners website the bushwhacker launches variety of attacking ways to block the communication services being carried out at different position and between colorful factors inside the system the bushwhackers aim to make vital coffers and services inapproachable to the authorized stoner of the system as well as the effectiveness of similar communication is also planned to be thrashed the study of literature of dos attacks signifies that the identification of similar bugs in the system may be an suggestion of probabilistic attack on the system so similar suggestion must be anatomized completely to fight the futuristic attack by the internal as well as the external interferers.

➢ 1.2 Rationale for ECC algorithm

Here are some advantages of utilizing ECC Certificates:

1.2.1 Enhanced Key Strength

ECC keys, despite their small size, have the same level of strength as larger RSA keys due to the algorithm used to produce them. To illustrate, a 256-bit ECC key is equal to a 3072-bit RSA key, while a 384-bit ECC key is equivalent to a 7680-bit RSA key. These strong but small keys enable encryption to remain ahead of computing power without the need to simply increase key length.

1.2.2 Reduced Certificate Size

Because ECC certificates have smaller key sizes, less data is sent from the server to the client during the SSL handshake. ECC certificates also require less CPU and memory, which improves network performance, making a significant difference on high-traffic or high-volume websites.

II. AES ALGORITHM

The symmetric key cryptographic algorithm also known as the AES (Advanced Encryption Standard) uses the same key for both encryption and decryption. When storing sensitive data on a device or server, for example, AES encryption is frequently used to protect the data while it is at rest. With a block size of 128 bits and key sizes of 128, 192, or 256 bits, AES is based on the Rijndael cipher. Secure communication, file encryption, and disk encryption are just a few of the many uses for AES.

Data can be encrypted and decrypted using the symmetric key encryption algorithm AES. Data at rest encryption and decryption using AES is very popular.

The suggested scheme primarily operates by merging the ECC and the Advanced Encryption Standard (AES) technique to guarantee validation and information coherence.

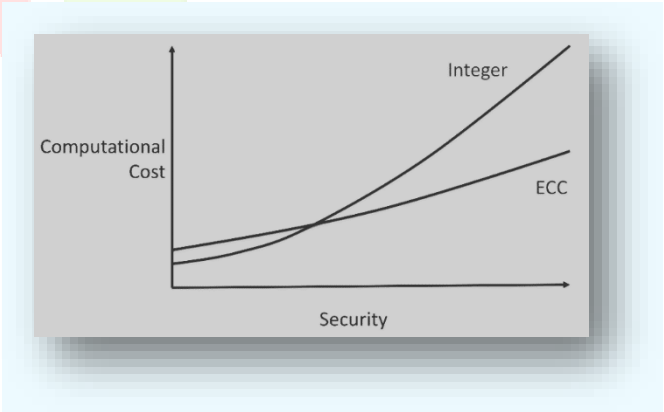

Fig.2: - ECC Efficiency at High Security

III. EXISTING SYSTEM

The RSA algorithm is currently the most popular public key cryptography algorithm used by many vendors for encryption and decryption. The first-generation algorithm used to provide data security is this one. Without exchanging a secret key separately, it can be used to encrypt a message. Digital signatures and public key encryption can both be performed using the RSA algorithm. Due to the difficulty of factoring large integers, it is secure. Without exchanging secret keys first, party A can send party B an encrypted message. The message is simply encrypted by A using B's public key, and B uses his private key to decrypt it. A can sign a message using their private key and B can verify it using A's public key when using the RSA algorithm to sign a message.

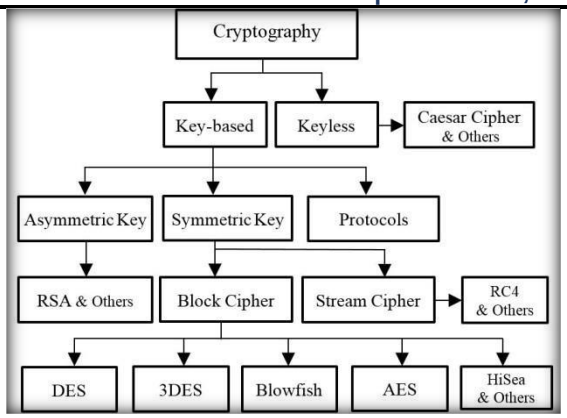

Fig.3: - Types of Cryptographic Encryption Algorithms

IV. PROPOSED SYSTEM

of five years. The time series monthly data is collected on stock prices for sample firmsand relative macroeconomic variables for the period of 5 years. The data collection period is ranging from January 2010 to Dec 2014. Monthly prices of KSE -100 Index is taken from yahoo finance.

Both clouds concur on a piece of known data. The elliptic group is computed from the elliptic curve equation, along with the following:

i. values of a and b

ii. prime, p

b. The elliptic group calculated from the equation for the elliptic curve

c. A base point, B is taken from the elliptic group.

4.1 Key Generation

1. A selects an integer dA. this is A's private key.
2. A then generates a public key i.e., PA=dA*B
3. In a similar fashion, B chooses a private key dB and generates a public key PB=dB *B.

A generates the security key as K= dA *PB.

4. B generates the secret key K= dB *PA.

4.2 Signature Generation

For signing a message m by the sender of cloud A, using A's private key dA.

1. Calculate e=HASH (m), where SHA-1 is an example of a cryptographic hash function called HASH.
2. Select a random integer, let us assume k from [1, n − 1]
3. In the case where (x1, y1) = k * B, determine r = x1 (mod n). Now go to step 2, if r = 0.
4. Determine the value of s = k 1(e + dAr) (mod n). Go to step 2 if s equals 0.
5. The letters (r, s) form the signature.
6. To cloud B, send your signature (r, s).

4.3 Encryption Algorithm

Let's say A wants to send B a message that is encrypted.

i. Using point PM from the elliptic group, A encodes plaintext message M.
ii. A then selects a second random integer, k, from the range [1, p-1].
iii. The cipher text consists of two points. PC equals [(kB), (PM + kPB)].
iv. Send cipher text to Cloud B using a computer.

4.4 Decryption Algorithm

The following steps will be taken by Cloud B to decrypt the cipher text PC:

a. B calculates dB. dB * (kB), which is the product of the first point from the PC and his private key. b. Secondly, B subtracts this result from the second point from PC (PM + kPB) - [dB(kB)] = PM + k(dBB) - dB(kB) = PM.

c. Using PM, B cloud uses the message, M, to decode it.

4.5 Signature Verification

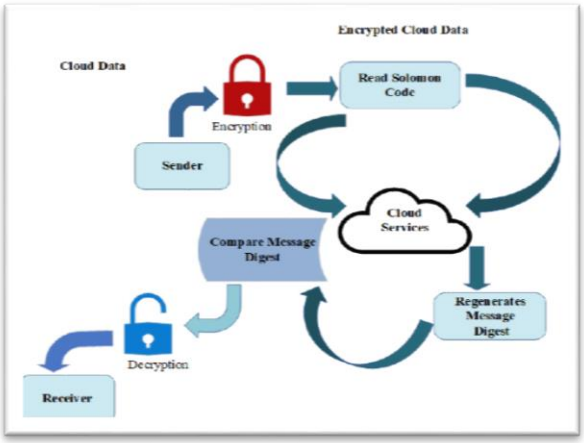

Fig.4: - ECC Cloud cryptography workflow.

V. CONCLUSION

This exploration composition proposes a new encryption algorithm for cloud computing- grounded systems. We have surveyed the research papers published in the last 10 years span and figured out around 100+ research papers through a single publication, viz. IEEE. The proposed algorithm has been anatomized with colorful algorithms like DES, AES, and Blowfish. The performance of the proposed algorithm has been compared with several parameters primarily including time for encryption for the colorful size of the blocks, the avalanche effect on the plain textbook which is 64 percent, and with the key is 57 percent. Compared to first-generation public key techniques like RSA, elliptic curve cryptography offers higher security and more effective performance in the world of cryptography. The elliptic curve alternative should be seriously considered by vendors looking to upgrade their systems because of the computational and bandwidth advantages they provide at a comparable level of security. Although the security of ECC has not yet been fully assessed, it is anticipated that it will soon be used extensively across many industries. The ECC has proven to have significantly fewer overheads than RSA after being compared to each other. Due to its ability to offer the same level of security as RSA while utilizing smaller keys, the ECC has many benefits. Its lack of maturity, however, may even hide its attractiveness because mathematicians felt that not enough research had yet been done on ECC. This research can be expanded to compare ECC to other algorithms used for key exchanges, digital signatures, and providing data integrity.

REFERENCES

1. Alowolodu O.D, Alese B.K, Adetunmbi A.O., Adewale O.S.” Elliptic Curve Cryptography for Securing Cloud Computing Applications.” Volume 66 No.23 Mar-13
2. Abdulkadir Abdullahi Ibrahima*, Dr. Wilson Cheruiyotb.” Data Security in Cloud Computing with Elliptic Curve.” Volume 26 No.1 2017, pp. 1 to 14
3. Ravi Gharshi, Suresha. " Enhancing Security in Cloud Storage using ECC Algorithm” Volume 2 Issue 7 July 2013, pp. 59 to 64
4. V. Vincy, Dr. B. Sathees Kumar.” A Comparison of ECC and Improved ECC Algorithm for Cloud Security.” Volume 3 Issue 6 Aug-18, pp. 501 to 507
5. Ankit Kumar Singh, Saroj Kumar, Abhishek Rai. “Secure Cloud Architecture based on YAK and ECC.” Volume 90 No.19 Mar-14: pp. 9 to 33
6. Vidyanand Ukey, Nitin Mishra.” Dataset Segmentation for Cloud Computing and Securing Data Using ECC” Vol. 5 (3) 2014, pp. 4210 to 4213
7. Mohammad Rasoul Momeni.” An Efficient Authentication Protocol for Mobile Cloud Environments using ECC” Vol. 15 No. 4. Jul-15, pp. 1694 to 2108
8. Kamyab Khajehei.” Secure Communication in Cloud by Using ECC Algorithm.” Vol. 3 No 1 14-Jan, pp. 1561-1565
9. T.Daisy Premila Bai.“ECC-based Security Architecture for IoT Cloud Integrated Smart Applications.” Volume 13 No 24 2018, pp. 16812-16818
10. Divya R Nair, Syam Gopi. “Third Party Public Auditing for Shared Data in The Cloud Using ECC.” vol. 7 Issue 8 Aug-17, pp. 01 to 05
11. Silki Jain, Abhilasha Vyas. “An Improved Security Framework for Cloud Environment using ECC algorithm” Vol 6. Issue 1 Jan-18, pp. 635 to 641
12. Siva Sankaran P, Kirubanand V B.” Hybrid cryptography security in the public cloud using two fish and ECC algorithm.” Vol. 4, Vol. 9, No. 4, Aug-19, pp. 2578 to 2584
13. A. Harsha and Basavaraj Patil. “Security of Data in Cloud Storage using ECC Algorithm.” Vol. 6 Special Issue Oct-16, pp. 143-146
14. Atanu Basu, Indranil Sengupta, and Jamuna Kanta Sing. “Secured Cloud Storage Scheme Using ECC Based Key Management in User Hierarchy.” 2011, pp. 175-189
15. Nasheem Khan, Vinod Kumar, Adesh Kumari. “An Identity-Based Secure Authenticated Framework by Using ECC in Cloud Computing.” Volume 4 Issue 2 Feb-15, pp. 605-608
16. Tien-Ho Chen, Hsiu-lien Yeh, Wei-Kuan Shih. “Advanced ECC Dynamic ID-Based Remote Mutual Authentication Scheme for Cloud Computing.” 2011, pp. 155-159
17. Antony Joseph Rajan D Naganathan E R. "Long and Strong Security using Reputation and ECC for Cloud Assisted Wireless Sensor Networks.” Volume 21 Issue 1. 2020, pp. 85–92
18. Adesh Kumari, Vinod Kumar, M. Yahya Abbasi, Saru Kumari, Pradeep Chaudhary, And Chien-Ming Chen. “Cloud-Based Secure and Efficient Framework for Smart Medical System Using ECC” Vol 8 June 4, 2020, pp. 107838-107852
19. S. Hendry Leo Kanickam and L. Jayasimman. “Comparative Analysis of Hash Authentication Algorithms and ECC Based Security Algorithms in Cloud Data.” Vol 8 no.1 2019 53-61
20. Parwinder Kaur Dhillon and Sheetal Kalra. "A secure multi-factor ECC based authentication scheme for Cloud-iot based healthcare services.” 2019, pp. 149-164
21. Dilip Venkata Kumar Vengala. “Three-factor authentication system with modified ECC based secured data transfer: untrusted cloud environment.” vol 1 no 3 16 February 2021
22. Bayu Anggorojati Neeli Rashmi Prasad Ramjee Prasad. “Capability-Based Access Control with ECC Key Management for the M2M Local Cloud Platform.”30-Dec-17
23. Jobandeep Kaur, Dr. Vishal Bharti, Mr. Shamandeep Singh. “Enhanced Hybrid Blowfish and ECC Encryption to Secure Cloud Data Access and Storage Policies.” Vol. 16, No. 5, May 2018 38-44
24. N. Bhaskar, M. V. Ramanamurthy, K. Jaya Sankar, CRK Reddy, Satyam Pulkam. “A High Secured ECC Based IoT Audiometric System for Cloud Based Dynamic Sensor Domain Environment.” Vol.12 No.11 10-May-21, pp. 1892-1897 "
25. Ramanjot Kaur, Tanmaya Mahandru. “Novel Approach of Cryptography by Hybridization of ECC and Diffie-Hellman with Blowfish Method in Cloud Environment.” Vol 179 No 22 18-Feb, pp. 41 to 44
26. Dhananjaya. V, Dr. Balasubramani.R. “Design and Analysis of high-security ECC based Cryptography by Holomorphic and data storage in Cloud.” Volume 9 No.2 Apr-20, pp. 1720 - 1728

27. Dr. S. Revathi. “Cloud Data Security Based on Fuzzy Intrusion Detection System with Elliptic Curve Cryptography ECC Using Non-Adjacent Form Naf Algorithm.” Vol. 10 Issue 11 2021 November, pp. 31 to 36
28. Dr. Edward Danso Ansong, Dennis Redeemer Korda, Dickson Kodzo Mawuli Hodowu. “An Enhancement of Data Security in cloud computing with an Implementation of Two-Level Cryptographic Technique, using AES and ECC Algorithm.” Vol 9 Issue 9 Sep-20, pp. 639 - 650
29. Ogunleye and Akinsanya. “Elliptic Curve Cryptography Performance Evaluation for Securing Multifactor Systems in a Cloud Computing Environment.” Vol 63 No 7 2022, pp. 3212-3224
30. Shynu P. G., Nadesh R. K., Varun G. Menon, Venu P., Mahdi Abbasi & Mohammad R. Khosravi.” A secure data deduplication system for integrated cloud-edge networks.”
31. Jia Cui, Yudong Qi, Bei Hong, Qinghua Chen. “Research on Cloud Computing Data Security based on ECDH and ECC.”
32. Dr.M.Gobi, Karthik Sundararaj. "A Secured Cloud Security Using Elliptic Curve Cryptography" 27th March 2015, pp. 141 - 144
33. Shreya Sambhaji Ranadive, Harshada Sanjay Sawant, Jayesh Ekanath Pinjarkar. “Secure File Storage on Cloud Computing Using Cryptographic Algorithm.” 20/04/2022
34. Abhishek Kajal, Gulshan "Enhanced Cloud Storage Security Using ECC-AES A Hybrid Approach" Vol 4 Issue 5 Aug-18 94-98
35. Tara Alimunisha, Kolli Nuka Raju. "Secure Big Data Storage and Sharing in Cloud Using ECC Algorithm" Vol 4 Issue 5 Apr-17, pp. 641-647
36. S. Sridharan and A. Arokiasamy. “Effective Secure Data Storage in Cloud by Using ECC Algorithm.” vol 25 1 2017, pp. 117-127
37. V.Gunasundhari, Mrs.M.Parvath. ” A Technical Survey On Cryptography Techniques In Cloud Computing Environment.” Vol-7 Issue-5 2021, pp. 1402-1411
38. D. Pharkkavi, Dr.D. Maruthanayagam. “Time complexity analysis of RSA and ECC based security algorithms in cloud data.” Vol 9, No 3 2018, pp. 206-213
39. K.Mythili, S. Rajalakshmi.”Enhancing Role Based Access Control with Privacy in Cloud Computing.” Volume 13 Issue 1 Jan-22, pp. 204-211
40. Payal Patel Rajan Patel, Nimisha Patel.” Integrated ECC and Blowfish for Smartphone Security.” 2015 Dec, pp. 210-216
41. D bikshapathi. "Performance of evaluation for AES with ECC in Cloud environment." volume-3, issue-10, 2016, pp. 67-73
42. Mohd. Akbar, Irshad Ahmad, Dr. Thirupathi. “Regular study and improved data storage in cloud computing using cryptography.” Volume 03 Issue 02 Feb-21, pp. 94-99
43. Sheetal Kalra, Sandeep Sood. "ECC-based anti-phishing protocol for cloud Computing services "Vol. 8 No.3, 2013, pp. 130-138
44. Xiaochun YIN, Zengguang LIU, Hoon Jae LEE. "An Efficient and Secured Data Storage Scheme in Cloud Computing Using ECC-based PKI" 2014, pp. 523-527
45. Mohammad Ayoub Khan, (Senior Member, IEEE), Mohammad Tabrez Quasim, (Senior Member, IEEE), Norah Saleh Alghamdi and Mohammad Yahiya Khan “A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data.” Vol. 8 2020, pp. 52018-52027
46. U. Sujatha, U. Saranya and C.P. Boopathy. "Use Of Attribute-Based Encryption for Secure Data Access Control In Mobile Cloud Computing." volume: 01, issue: 01 2019, pp. 32-36
47. G.O.Ogunleye, S.E.Akinsanya. “Elliptic Curve Cryptography Performance Evaluation for Securing Multifactor Systems in a Cloud Computing Environment.” Vol. 63, No. 7 2022, pp. 3212-3224
48. Deepika Bhatia And Meenu Dave. "Elliptic Curve Layered: A Secure Polyalphabetic Vignere Cryptographic Algorithm for Textual Data.” Volume 65 Issue 1 2021, pp. 222-229
49. Ali Kadhim Bermani, Mehdi Ebady Manaa, Ahmed Al-Salih. “Efficient cryptography techniques for image encryption in cloud storage.” Vol 8, No 3 2020, pp. 1359-1373
50. "Balasubramanian Prabhu Kavin and Sannasi Ganapathy. "A New Digital Signature Algorithm for Ensuring the Data Integrity in Cloud using Elliptic Curves. "Vol. 18, No. 2, Mar-21, pp. 180-190