www.ijiarec.com

ISSN:2348-2079

Volume-7 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Towards efficient ECC based provable data possession protocol with data dynamics for secure cloud storage

E.P.Kaushik[1], P. Boobalan[1], K. Dhamodaran[1], S. Karthik[1], S. Prabhu[2]

[1]UG Students, Department of Computer Science and Engineering, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India

[5]Assistant Professor, Department of Computer Science and Engineering, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India

ABSTRACT

Distributed computing is familiar for its financially on-request benefits dependent on web. The critical advantages of cloud administrations drive associations and people to make roughage by re-appropriating information to cloud stockpiles. Re-appropriating information brings clients' a simple and conservative method for information the executives and furthermore soothes clients' from the weight of building and keeping up neighbourhood information stockpiling. Be that as it may, information being living in some outsider's premises, clients have no full command over their information which requires guaranteeing classification and uprightness of information put away in untrusted distributed storage servers. To check the accuracy of information in distributed storage, this paper proposes an effective ECC based Provable Data Possession (EPDP) Protocol with information elements. The proposed convention jam secrecy of information put away in distributed storage and enables information proprietor to check the honesty of information without recovering the entire unique information. Additionally the convention is intended to perform stateless evaluating and backings information elements at square dimension holding a similar security confirmation. Security and Performance examination ends up being secure and exceptionally proficient for secure distributed storage.

Keywords- Privacy, Cloud information stockpiling, Information honesty, Elliptic bend cryptography, Respectability check, Secure capacity

INTRODUCTION

Distributed computing has been imagined as a processing model that empowers pervasive, helpful system get to, area autonomous asset pooling, quick versatility and on-request self-administration that can be provisioned and discharged with negligible administration exertion or with specialist organization association [1]. The administration rendered by cloud that can't be contrasted and different models contains adaptability, adaptability, multi-occupancy, Device and Location Independence, spryness, pay for what you use and so forth. The real cloud specialist organizations like Amazon [2], Google [3] offer these attributes as administrations over the web. Other such suppliers incorporate Rack space, Microsoft, Sales drive, VMware, Verizon, Citrix, IBM [4, 10] and so forth. Moving information into distributed storage gives information proprietors an extraordinary accommodation which assuages proprietors from specialized complexities and from the weight of contributing, fabricating and keeping up claim foundation. Despite the fact that the advantages of cloud are critical and enormous, one of a kind viewpoint that obstructs the reception of cloud by numerous people and ventures is worry over information security [11]. Guaranteeing

Author for correspondence:
Department of Computer Science and Engineering, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India

privacy and honesty of the redistributed information is essential since information are put away on shared servers at remote site. As data are dealt with by certain untouchables, the data owner has nonattendance of full specialist over the redistributed data. Classification can be accomplished by scrambling the information utilizing industry standard calculations before moving into distributed storage. What's more, to avoid unapproved access, verification and access control conventions gives best arrangements. To get fine-grained access to redistributed information a safe convention is proposed in [12]. To use productively the pool of cloud administrations without dread, information proprietor must guarantee that the redistributed information isn't altered and are taken care of as they anticipate. To guarantee the rightness of put away information, information inspecting administration is basic. Numerous specialists have proposed plans for classification and uprightness check [13]-[24] for secure remote information stockpiles. Be that as it may, information uprightness confirmation can't be benefited as an administration from cloud suppliers since the cloud information stockpiles are viewed as untrusted servers. Subsequently it is one of the basic obligations of information proprietors to review how their touchy information are dealt with in cloud condition. Guaranteeing respectability of information is a troublesome assignment without a duplicate of information put away in information proprietor's server. Without having a neighborhood duplicate and recovering entire information from distributed storage for respectability confirmation ends up bulky for information proprietor. Consequently, a safe and proficient remote information honesty confirmation convention fulfilling the above prerequisites is required to get the affirmation that the redistributed information are taken care of obviously by information proprietors.

Ateniese et al. [25] was the first to present secure and proficient Provable Data Possession (PDP) plans dependent on homomorphic obvious labels. Wang et al. [26] structured a Privacy-Preserving Public Auditing for cloud information stockpiling in which open key based homomorphic authenticator was used and arbitrary concealing was utilized to accomplish protection safeguarding open reviewing plan. Yang et al. [27] has proposed PDP for asset compelled cell phones in cloud utilizing bilinear mark and Merkle Hash Tree. Zhu et al. [28] developed an intelligent PDP convention dependent on Diffie-Hellman calculation. Natu and Pachouly [29] has looked at different PDP plots and has turned out with points of interest and burdens of different plans. Liu et al. [30] has proposed an open examining plan dependent on BLS short mark strategy and homomorphic hash work. Worked at [31] proposed a Privacy-safeguarding open inspecting plan in which the disadvantage of Wang et al's. plot has been survived. Vanitha et al. [32] has structured a Privacy-saving open inspecting plan dependent on elliptic bend computerized mark calculation for the mutual information in cloud. The processing labels for the information and re-appropriates information document and labels into distributed storage. Later the information proprietor or a depended outsider evaluator can send a test to cloud server to check the honesty of information. The server thus has to demonstrate that the ownership of information is protected by creating a proof for the test with the put away information and labels. Finally verifier can check the confirmation to check uprightness of information. Since the re-appropriated information are liable to updations, the proposed convention is intended to help information dynamics moreover. The proposed EPDP convention underpins information tasks, for example, addition, erasure and adjustment at block level. Additionally the proposed framework is thought to be stateless, implies that the verifier need not keep up states between all reviews which is viewed as an alluring property in a n examining framework. All in all the proposed EPDP convention offers affirmation to information proprietors that their re-appropriated information are dealt with as they anticipate. Whatever is left of the paper is sorted out as pursues: Section II depicts the System Model, Section III explains the proposed Provable Data Possession ace tool, Section IV manages Data elements, Section V examines Security and Performance investigation, and Section V I closes with end.

SYSTEM MODEL

Cloud Data Storage overview

The cloud condition and the staggered security framework required to ensure the information put away in cloud servers and the duties of an information proprietor in securing information are talked about thoroughly in [33]. The cloud information stockpiling model considered in this paper comprises of the accompanying substances as portrayed in Fig.1.

1. Data Owner (DO): a substance that redistributes information to cloud information stockpiling.
2. Data User (DU): an approved individual who sends ask for getting to the information put away in distributed storage.
3. Cloud Service Provider (C SP): an element that gives stockpiling as an administration to clients.
4. Third Party Auditor (TPA): a discretionary element, aptitude in checking the honesty of the redistributed information for the benefit of information proprietor.

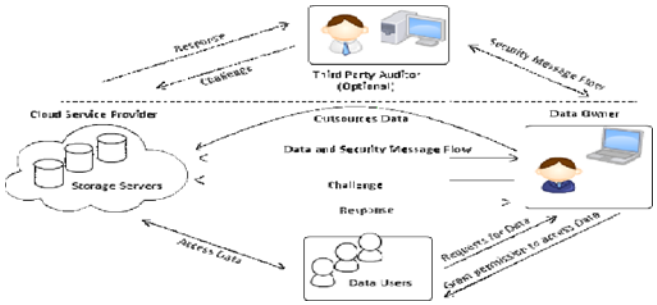


Fig. 1. Cloud Data Storage overview

Security Attacks

The information proprietors are prescribed to encrypt information before redistributing so as to ensure the sensitive information facilitated to cloud servers. Despite the fact that the information are scrambled, an assailant who is keen on knowing the information if impractical to decipher it, might decimate the put away information by doing a few controls or may erase a few information which results in perplexities to information proprietor. At such time there is a basic requirement for a productive information trustworthiness check instrument which helps in confirming whether the put away information is flawless. This information trustworthiness verification should be possible by information proprietor without anyone else or can appoint a trusted TPA to play out the confirmation. The two sorts of dangers in distributed storage condition are as per the following:

Internal Attack

The special clients in the CSP site realize how to deal with the put away information and consequently may either deliberately or accidently control or break information which results in substantial misfortune to information proprietor.

External Attack

The malignant clients from outside the cloud condition may bargain cloud servers and hacks information which may influence the two information proprietor and CSP.

Design Goals

The proposed framework is aimed in planning an honesty confirmation convention that is effective and sufficiently secure to check the information put away in distributed storage. The proposed EPDP convention ought to include the accompanying properties:

Security

The proposed convention ought to guarantee classification and trustworthiness of the re-appropriated information. Classification implies the information is ensured utilizing encryption procedures and just approved clients should get to the secured information and Integrity implies

checking whether information has experienced unapproved manipulations.

Stateless check

The verifications produced by the convention ought to be founded on haphazardly picked difficulties which relieve verifier from keeping up states between reviews.

Efficiency

The proposed convention ought to be productive as far as low calculation and capacity overhead and the challenge presented ought to be boundless which genius the effectiveness of the proposed convention.

Audits without downloading

Data honesty confirmation ought to be managed without recovering the duplicate of entire unique information.

Key Generation – given a security parameter as information, this calculation creates a key pair (mystery key, open key) as yield.

Tag Generation– given information square, utilizing a hash work and keys as data sources, this calculation gives labels as yield.

Challenge Generation – choosing arbitrary qualities, this calculation produces test (challenge) as yield.

Proof Generation – given a test 'challenge' stored information document and labels as sources of info, this calculation creates a proof for information ownership as yield.

Proof Verification– given created proofs challenge and mystery key as sources of info, this calculation checks the evidence of information ownership and produces acknowledge or dismiss as yield.

Pre-Processing Phase

To guarantee classification of the redistributed information, before moving information into distributed storage it must be scrambled utilizing industry standard encryption calculations. In light of the affectability how information could be ensured through staggered security framework and how information clients in a chain of command could get to these ensured information securely are examined in [33, 12]. The encoded information document is considered for preparing in the proposed framework. The periods of the proposed EPDP convention are as per the following:

Key Generation phase

The key age calculation, 'GenKey' is executed by information proprietor to create mystery and open key pair. For a given security parameter k, the GenKey calculation gives a mystery and open key pair (sk, pk) as yield. Information proprietor chooses an irregular whole number k from [1,n-1],and P=kG is registered, where k is the mystery key and P is the open key.

Algorithm 1: GenKey

1. Procedure: GenKey(1^k)→(sk,pk)
2. select a random integer k ϵ [1,n-1]
3. compute P=kG
4. sk← k, pk←P
5. End Procedure

Tag Generation phase

The information proprietor registers labels over the encoded information records by executing Tag age calculation 'GenTag'. For producing labels, the information document F is partitioned into squares, state F = m1, m2,...,mn . For each square mi, in information document, information proprietor chooses an irregular number di from [1,n-1] as the mystery esteem (sv) of the square for which label Tm is created. The mystery key(sk) and the directions of open key(pk) are utilized in figuring the labels. Alongside these keys a hash work h:{0,1}*→Zp and the square mystery esteem (sv) are utilized in label calculation. The information document and the produced labels for the information squares {F, Tm}are sent to CSP.

Algorithm 2: GenTag

1. Procedure: GenTag(m,sv,sk,pk)→T_m
2. compute $\sigma_{i,1}$= h(m_i)k d_iP_x
3. compute $\sigma_{i,2}$= d_iP_y
4. T_m←{$\sigma_{i,1}$,$\sigma_{i,2}$ }
5. End Procedure

Challenge Generation phase

Information proprietor can confirm the honesty of the information put away in distributed storage by testing CSP. The verifier makes a test by executing test age calculation 'GenChal' and sends it to server for verification generati on. To produce

a test, verifier chooses I={a1, … ,a c}, an arbitrary c-component subset of the set [1,n] and for each i∈ I (1≤i≤c), an irregular esteem ri is picked. The test 'chal' shows the positions and the obstructs that are to be confirmed and is spoken to as chal={(i,ri)}i∈I . The server on getting 'chal' from the verifier, figures the reaction for the test and returns it to the verifier.

Algorithm 3: GenChal

1. Procedure: GenChal (k)→chal
2. Choose a random c-element subset I from the set [1,n]
3. For each i∈ I, 1≤i≤c,

a. select a random value r_i

b. chal←$\{(i,r_i)\}_{i\in I}$

c. End Procedure

Proof Generation phase

The CSP on accepting a test from the verifier, registers a relating reaction as information trustworthiness verification. The calculation 'GenProof ' is executed by CSP which takes the information record, labels, challenge 'chal' and open ke y as data sources and produces ρ ={τ,μ) as confirmations.

Algorithm 4: GenProof

1. Procedure: GenProof(F,$\sigma_{i,1}$,$\sigma_{i,2}$, chal, pk)→ρ
2. compute $\tau = \prod_{i=a}^{ac} 1^{\sigma i,1} {}^{P}y^{r_i}$ A
3. compute $\mu = \prod_{i=a}^{c} 1\,\sigma_{i,2} hm_i P_x r_i$
4. ρ ←{τ,μ}
5. End Procedure

Proof Verification phase

Information proprietor on accepting the reaction for the test from the CSP, confirms the honesty of the information by executing confirmation check calculation 'Check Proof'. Verifier veri fies whether the accompanying condition holds for the got reaction utilizing his mystery key. Check Proof calculation takes the reaction ' ρ', challenge 'chal' and mystery key(sk) as sources of info and returns 'genuine' if the trustworthiness of queri ed information squares are confirmed as right or returns 'false' o therwise. That is, the verifier can check for the condition τ = k μ. In the event that the condition holds, at that point the yield is "genuine" false.

DATA DYNAMICS

The proposed EPDP convention bolsters different activities, for example, addition, change and erasure on squares in the information record.

Block Insertion (BO=1)

The information proprietor guess needs to embed a square in a predefined position say, after square 'p' in the information document F, at that point calculation 6 is executed to complete the work. In the proposed framework, the square addition activity can be performed without figuring again the labels for the squares which are gone in reverse because of inclusion of another square.

Algorithm 6: Block Insertion

1. Procedure: Block Insertion←(p,m^*_k
2. Select position p and new block to be inserted,
3. m^*_k
4. Compute $\sigma_{k,1}$,$\sigma_{k,2}$
5. T_k←$\sigma_{k,1}$,$\sigma_{k,2}$
6. Send request to server to process the update, ProcessUpdateRequest(1,p,m^*_k ,T_k)
7. End procedure

Block Modification (BO=2)

The information proprietor guess needs to embed a square in a predefined position say, after square 'p' in the information document F, at that point calculation 6 is executed to complete the work. In the proposed framework, the square addition activity can be performed without figuring again the labels for the squares which are gone in reverse because of inclusion of another square.

Algorithm 7: Block Modification

1. Procedure: Block Modification←(p,m^*_k
2. modify block$m_p$to m^*_k
3. Compute $\sigma_{k,1}$,$\sigma_{k,2}$
4. T_k←$\sigma_{k,1}$,$\sigma_{k,2}$
5. Send request to server to process the update, ProcessUpdateRequest(2,p,m^*_k ,T_k)
6. End procedure

Block Deletion (BO=3)

The information proprietor guess needs to erase a square say, mp in the information document F, at that point calculation 8 is executed to perform erasure. When server erases the predefined

obstruct, all other ensuing squares are pushed ahead one stage which is the turn around procedure of square inclusion.

Algorithm 8: Block Deletion

1. Procedure: Block Deletion ←(p
2. Select block m_p to be deleted
3. Send request to server to process the update, ProcessUpdateRequest(3,p)
4. End procedure

Process Update Request

The information activities get finished with the Process Update Request calculation. Every datum activity ask for thus calls process refresh calculation to finish the errand. This calculation at last updates obstructs in server as indicated by the square task ask for send by the information proprietor.

Algorithm 9: Process Update Request

1. Procedure: Process Update Request→F
2. If BO=1 then
3. Insert m^*_k after m_p and move all blocks after m^*_kbackward
   i. Store the corresponding tag T_k in server
4. Else if BO=2 then
   i. Update block m_p with m^*_k
   ii. Store the corresponding tag T_k in server
5. Else if BO=3 then
6. Delete block m_p and tag T_p
   i. Update file F to F'
   ii. Return(F')

SECURITY AND PERFORMANCE ANALYSIS *A. SECURITY ANALYSIS*

This area talks about the security examination of the proposed convention. The proposed EPDP convention is turned out to be right and is likewise solid.

Correctness

Theorem: In the event that the re-appropriated information is put away genuinely in distributed storage server, at that point at whatever point the server gets a test from verifier could register confirmation for the test that will dependably be acknowledged by the verifier.

Proof: We have

$\tau = \prod^{ac} \sigma_{i,1} P_y r$

$i=a_1$ $_i$

a_c

$=\sigma i,1^P y^r i$

$=a_1$

a_c

$= (hm_i kd_i P_x)\ P_y\ r_i$

$i=a_1$

a_c

$= (\ \sigma_{i,2}\ hm_i\ kP_x\ )\ r_i$

$i=a$

$_1$

a_c

$= k\ (\sigma_{i,2}\ hm_i\ P_x\ r_i)$

$i=a_1$

$= k\ \mu$

From the above confirmation the proposed convention is said to be right or legitimate.

Soundness

***Theorem*:** For the exploitative server it is infeasible to bewilder the verifier to acknowledge a bogus confirmation. ***Proof*:** The server after using the as of now registered esteem or the speculated esteem can't perplex the verifier in tolerating a bogus verification on the grounds that each time the test is picked haphazardly.

Performance Evaluation of Probabilistic verification

The proposed convention permits distributed storage server to demonstrate information ownership of chose squares of information document F. This nature of testing identifies server rowdiness with high likelihood and furthermore diminishes the remaining burden on capacity server. Following are the suppositions utilized for location likelihood.

- Out of n squares of information record F, server upsets d squares (d/n)
- Verifier arbitrarily chooses the records is uniform and subsequently likelihood of choosing any square in the information document F is 1/n.
- Verifier approaches evidence for a test which by and large has 'c' distinctive squares and recognizes rowdiness with high likelihood.

The recognition likelihood P is as per the following:

$d^{\ c}$

$P = 1 - (1 - {}_n)$

$\text{wherec} = \log(1 - P)$

P determines the location likelihood that, if server disturbs 'd' shut out of 'n' squares of the information document F, the verifier can recognize the interruption when a test is send for which the server needs to register confirmation for 'c' squares. Fig .2 plots P for consistent estimation of d and for various estimations of n and c. It demonstrates the outcome for various location likelihood from 0.5 to 0.99.

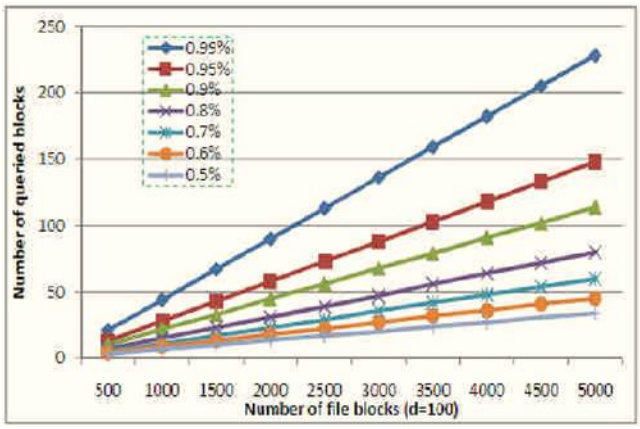
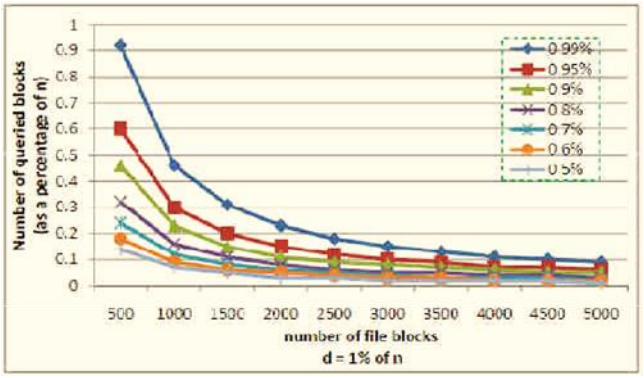


Fig. 2. Server misbehavior under different detection probability– number of data file blocks (n), number of queried blocks (c), disrupted block (d=100 blocks)

Fig.3 portrays the adjustments in proportion under various location probabilities where the quantity of upset squares is 1% of n. The verifier, to accomplish P of 99% ought to request least 458 squares for confirmation. To accomplish P of 95%, 90%, and80%, the verifier ought to request something like 298, 229 and 160 squares for check individually.



Performance Evaluation

The execution of proposed EPDP convention is talked about in this area. Table II demonstrates the documentations utilized for assessment of cryptographic activities. The convention is assembled utilizing cryptographic hash work and elliptic bend cryptography. On the information proprietor side, a couple of keys are produced and are utilized in label age. The calculation cost for this procedure is nThash + 4nTmul + T, where n is the quantity of record squares. On the server side, confirmation is created and sent to verifier for trustworthiness check. The calculation cost for this procedure is cThash + 5cTmul. After accepting confirmation for the questioned squares, verifier assesses the evidence for uprightness check. The calculation cost for this procedure is cTmul, where c is the quantity of questioned squares. An examination between plans proposed in [26], [30]

and the proposed EPDP convention is as per the following: To check the effectiveness of the proposed convention, the recreation is performed utilizing Intel Core i3 processor with 4GB RAM and Java cryptography library is utilized. The plans proposed in [26] and [30] depend on bilinear blending which includes calculation cost for augmentation activity, exponentiation tasks and bilinear sets. Since the proposed EPDP convention is worked without matching, the calculation cost for example tasks and bilinear sets are decreased and the calculation cost for measured augmentation, elliptic bend point increase and hash capacities are included. The examination is performed, state the quantity of questioned squares c = 32 and the calculation expenses of the convention in [26, 30] and the proposed convention are appeared in the accompanying Fig.4.

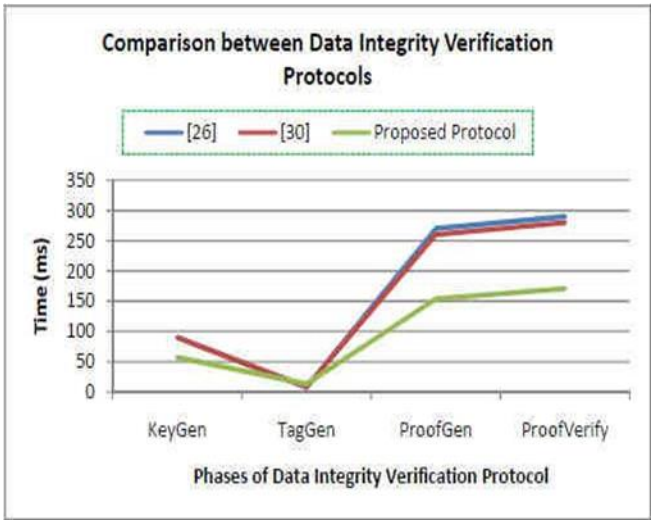


Fig. 4. Comparison between [26, 30] and the proposed protocol

Fig.4 portrays the calculation cost for every calculation in [26], [30] and the proposed EPDP convention. From the examination, it is resolved that the calculation cost is limited and in this way the correlation result demonstrates the effectiveness of the proposed convention.

CONCLUSION

The Cloud Computing worldview gives clients various significant administrations that are required in the present worldwide electronic town. The most generally utilized cloud administrations incorporate information stockpiling and registering administrations. Information proprietors facilitating touchy information in distributed storage servers need to beat information security issues. To guarantee privacy and trustworthiness of information redistributed to distributed storage, in this paper, a productive provable information ownership convention utilizing elliptic bend cryptography is proposed. The information proprietor can perform stateless evaluating to check the rightness of information put away in cloud. The uprightness check should be possible without recovering the entire unique information from cloud server which limits correspondence overhead. Additionally the proposed convention bolsters dynamic information activities at square dimension keeping up a similar security confirmation. Through security and execution investigation it is demonstrated that the proposed convention is secure and effective as far as privacy and trustworthiness.

REFERENCES

[1]. P.Mell and T.Granc ”Draft NIST working definition of cloud http://csrc.nist.gov/groups/sns/cloudcomputing/index.html.2012
[2]. Microsoft Azure, (online), available, http://azure.microsoft.com/en.in.
[3]. Sales force, (online), http://www.salesforce.com/en.in.
[4]. VMware cloud, (online), available, http://vcloud VMware.com/en.in.
[5]. Verizon, (online), available, http://www.verizonwireless.com/support/verizoncloud.
[6]. Citrixcloudservice,(online),available,http://citrix.com/solutions/cloudservice.
[7]. IBM cloud, (online), available, https://www.ibm.com/cloud computing.
[8]. D.Sudhadevi and T.Thilagavathi “a novel approach to enhance cloud data defense” Asian journal of information technology, 12(9), 2013, 305-311.
[9]. D.Sudhadevi,T.Thilagavathi ”an elliptic curve cryptography based adaptive and secured protocol to access data outsourced to cloud server”, international journal of engineering research, 10(18), 2015.