Performance Improvement of MONCRYPT SSA Over Data Obfuscation in Cloud Security

D. Samatha, D.Sindhura, K.Kalpana, T.Santhi sri

Abstract: Cloud computing means a set of Information Technology services offered to the users over the web on a rented base. Cloud computing has several benefits like pliable, planning, scalability, combination, and rebate .Security is one in every of the most challenges that hinder the expansion of cloud computing. This study introduces a brief analysis of the issues and challenges of cloud computing security. "Cloud computing services will be varied and must be defined from the perspective of the users of the service. Security of information keep within the cloud is most imperative test publically cloud setting. Due the security issues, information are uncovered by Cloud Service Providers (CSP) and others clients of cloud. To verify the information from security lapse, we are using Security Algorithm , named MONcrypt SSA to protect the data in cloud depository . The proposed technique is depend on information jumbling strategies. The MONcrypt SSA depends on Security as a Service (SEaaS). In this we can utilize the JAVA to recreation of results is utilized for measure the security of propose and existing jumbling procedures. MONcrypt contrast and present jumbling procedure that is Base64Encoding .The anticipated strategy gives better and shrewd security in examination with present obscurity strategies. Not at all like present system, MONcrypt diminishes the size of information that will be transferred in distributed storage.

Keywords: Security service algorithm, obfuscation , MONcrypt SSA , Encoding

I. INTRODUCTION

Cloud Computing is that the observe of employing a net of far servers hosted on the net to store, manage, and method information, instead of an area server or a private laptop.

It is evolved from Grid computing, parallel computing and distributed computing. It has a policy known as pay as u use. It provides on-demand services. The main issue focused in cloud computing is data security. Now a days security in cloud has become a real challenge in public cloud condition. include for accounts in cloud had gotten more as each one are moving their information on to cloud for privacy, unwavering quality and effectiveness. Because of numerous security issues information in revealed by cloud specialist organizations and other unapproved clients of cloud. To verify the information from informal clients we proposes a private system which is known as MONcrypt SSA to secure the information in cloud. This

private method is expand on Data obscurity system.Data obfuscation technique is also named as Data Masking. To explain fully about data masking and its enterprise potential we first needs to understand how it works. As name only says data masking also know as data obfuscation which means hiding original content with modifies content .

Data masking could be a technique of making a structurally similar however counterfeit version of associate organization's information which will be used for functions like code testing and usercoaching. The purpose is to guard the particular information whereas having a purposeful substitute for occasions once the important information isn't needed. In information masking, the arrangement of data stays the same, only the values arechanged. Data could also be altered in an exceedingly variety of how, which includes encryption, character dearrangement, and letter or word substitution.. The current muddling procedures are Base32 Encoding, Base64 Encoding and Hexadecimal encoding. MoNcrypt SSA gives more desirableperformance and greater quality security when contrasted with existing jumbling strategies. Information muddling is like encryption. The principle contrast among encryption and information jumbling is in encryption even extreme we realize the calculation finding the mystery key is troublesome and when coming to obscurity realizing the calculation is difficult.Basically, confusion is totally unique in relation to encoding from numerous points of view. Basically, it needn't bother with any converse change. Next, it's a bit much for partner attacker to show up for the main code constantly, because of the assault are regularly succeed while not having the principal code of thecode. For examining a code, any dis constructing agents or is expected to use on the executable code. However, clearly the dismantled code will be not like the first code, as it is beyond the realm of imagination to expect to get back with every single same usefulness. As the majority of the code investigation methods have been inquired about and probed Assembly code or with low level code; along these lines, Assembly level writing computer programs is considered in this paper. In the following area, not many obscurity strategies are discussed.Data stockpiling and observing are the most significant undertakings for all endeavors.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author

D.Samatha, Department of CSE, Koneru Lakshmaiah Education Foundation, A.P, India.
D.Sindhura, Department of CSE, Koneru Lakshmaiah Education Foundation, A.P, India.
K. Kalpana, Department of CSE, Koneru Lakshmaiah Education Foundation, A.P, India.
T.Santhi sri, Department of CSE, professor at Koneru Lakshmaiah Education Foundation, A.P, India.

Little and Medium scale Enterprises (SME) are not having enough foundation to do as such. Distributed computing tackles this issue by giving huge virtual storage12. SMEs re-appropriate the information to distributed storage.

The essential meaning of redistributing is to move the in-house exercises to the outsider (cloud supplier) who has the necessary skill to perform information support exercises in a powerful and effective manner.

Different purposes behind redistributing information are to access the information and to lessen the dangers related. This marvel has helped SMEs focus more on its center abilities and subsequently to increase upper hand in themarkets.

Information re-appropriating makes numerous security issues on the put away information in cloud. Expert began utilizing confusion procedures to give security to the information in cloud. To keeping up security for the re-appropriated information in cloud is a basic errand. To improve the security of information, MONcrypt SSA is proposed for verifying numerical information. As a section this examination, there is a SSA called AROcrypt13whichis utilized for Non-numerical information. Clients can utilize these two SSA dependent on their touchy information. AROcrypt is utilized forNon-numerical.

II. PROBLEM DEFINITION

Information security is a difficult undertaking in cloud condition. Cloud is boundless, and the information can be physically put at any server farms which are topographically conveyed. Henceforth CSP knows everything about our information and where our information is found and he can get to our information. Clients' information sent to the cloud will be under the influence of CSPs. CSPs as advantaged overseeing chief reserve the privileges to investigate the clients' information. Along these lines, there is a likelihood that information are hacked from CSPs. Since distributed storage don't have any confinements, information stockpiling in cloud isn'tcontrolled. Consequently, information of one client may consolidate with the information of another client as cloud is an open domain. Clients does not have any thought regarding encryption in cloudstorage.Maintaining keys for each user is more difficult for CSPs,andthe same key is utilized for all clients' data20. Clients' information must be in a fixed arrangement determined by the CSP, and henceforth the CSP realizes all the data required for understanding clients' information.

III. LITERATURE SURVEY

Dr. D. I. George Amalarethinam [1] proposed plain text and an image that to be stored in cloud storage using Data obfuscation .He uses a method called Steganography which means the ordinary data will be hidden by secret data, non-secret, file or message in order to avoid detection .Author had given a pseudo code for plain text as well as an image. In this code he had used MRADO Technique. The MRADO Technique improves classical obfuscation techniques by integrating substitution, transposition and ASCII values. He also derived some formulas for this technique.

S. Arul Oli1 [1] proposed how Data obfuscation techniques are used in encryption as well as decryption. Author proposed a Data obfuscation technique Pseudo code in java and got cypher text from plain text as well as plain text from cypher text by de-obfuscating the data. Author had given a brief about the performance comparision of obfuscation techniques among themselves and had given a graphical comparision of 4 obfuscation technique.

S. Monikandan [1] proposed about the Data obfuscation techniques like Base64, Base32 Encoding, ANCII Encoding, Hexadecimal Encoding and explained in brief about this techniques with examples. Using this Data obfuscation techniques to store data securely in cloud does not give high performance .To give high performance regarding time and size we have used MONcrypt SSA algorithm. This paper contains pseudo code for MONcrypt SSA and explains this algorithm using an example. This paper also shows the graphical representation of performance comparision by obfuscation time. Su Qing proposed an answer to cross platform drawback regarding the obfuscation in C/C++ ASCII text file, and describe the principle and execution of source code muddling calculation. They arelayout confusion, information stream jumbling .

ChengyuHu[1] proposed Public-key secret writing using keyword search (PEKS) permits users to go looking on encrypted information, which is relevent to the scheme of sharing data in the utilitystorage. In this author centre on how to build a PEKS scenario viaobfuscation. Our basic theme is constructed on the differing-inputs obfuscation (diO) and may be thought-about as AN initial conceive to apply diO within the PEKS field. The theme supports looking out on encrypted information by providing to the cloud server AN obscure straightforward “decrypt-then-compare” circuit with the key and also the quiz keyword hardwired in it .

Levent Ertaul[1] proposed a new obfuscation algorithm based on Discrete Logs to Pack the Words and another one, based on Affine Ciphers, to Encode String Literals. Finally, author conclude this paper identifying the need for reviewing the performance of the algorithms as the future scope of thework.

Jean-Marie[1] focuses on metamorphic viruses. More exactly, it examines the use of advanced code obfuscation techniques with respect to metamorphic viruses. In explicit, author proves that reliable static detection of a specific category of metamorphic viruses is N P- complete problem. Then we have a tendency to by trial and error explain our result by constructing a sensible obfuscator that may well be utilized by metamorphic viruses within the future to evadedetection.

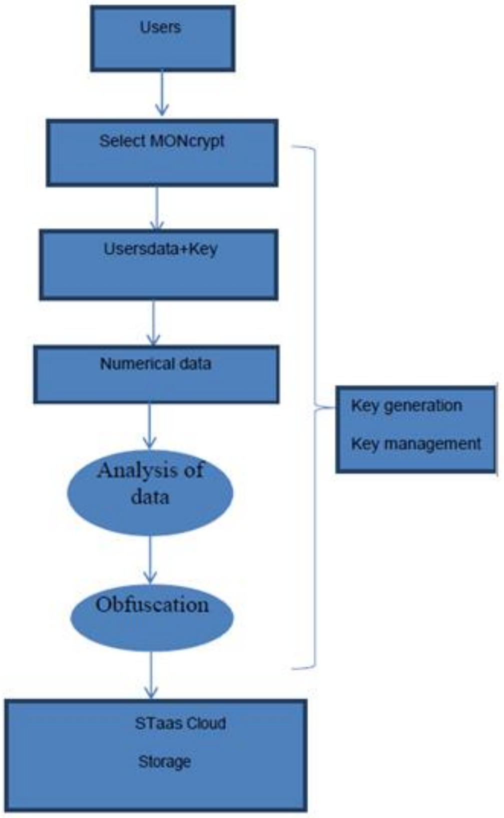
IV. METHODOLOGY

Distributed storage has gigantic measure of virtual extra room. It is utilized by a huge number of clients consistently. Re-appropriated information in utility stockpiling should be shielded from unapproved get to. MONcrypt is one of the SSAs gave via SEaaS. Figure shows the system chart of MONcrypt SSA.

There are three cloud administrations utilized for Security, K ey Generation and Management and Cloud Storage. These administrations are given by three distinctive free CSPs.

The information which are to be re-appropriated should be jumbled before they transmit to the utility stockpiling. It is executed when clients pick this SSA for information security. It utilizes scientific capacities to jumble the information, for example, pow(), switch(), module() and ascii(). Key indicates the quantity of pivot during muddling process. Key utilized for MONcrypt is created from Key Generation and Management as a Service (KGMaaS). Clients utilize the keys and MONcrypt SSA to muddle the information. The keys utilized for muddling are kept by the clients. It isn't conveyed to theCSP.

V. FLOW CHART



VI. DATA OBFUSCATION TECHNIQUES

Definition:-It is same as encryption but in this data obfuscation knowing the algorithm is very difficult to decrypt but knowing secret key is easy . It is quite opposite to the definition of Encryption .

Techniques:- Base32 , Base 64 Encoding , Hexadecimal.

a) ALGORITHM:

```
Obfuscation_text (PT)
Declaration
            PT -Plaintext
            S - Size of PT
            AC- ASCII codes of PT
            BIN -Binary code for AC
            BUFF- Buffer Variable
            K -Key for Bits Rotation
            RD -Rotated bits
            TC- Two's Complement

            N -Number of 8 bits binary
            BIT- 8 bits Binary
            DEC- Decimal value
            CT- Ciphertext
    1. Start

    2. S= size of(PT)

    3. for i=1 to S
            AC[i]=ascii(PT[i])
              BIN[i] =binary(AC[i])
          BUFF=append ( BIN[i])
        Next i
4.  Generate a key from cloudK

5.  for i= 1 to K
         RD= rotate (BUFF)
         Nexti
6.  TC=two-complement(BUFF)
7.   N=S/8
8.  for i=1 to N
            BIT[i]=div-bits(TC)
            DEC[i]=decimal(BIT[i])
            CT[i]=ascii(DEC[i])
            Next i
9.  CT=Ciphertext
End
```

BASE 64 ENCODING :

ENCODING ALGORITHM :

- We can download the any type of image toencode.
- First, importbase64
- Encoding the image we use function calledbase64.encodestring(S).
- Plain import base64 image=open('deer.gif','rb')
- Image_read=image.read()
  image_64_encode=base64.encodestring(image_read)
- Printimage_64_encode

DECODING ALGORITHM :

- Base64.decodestring(S)
- Base64.decodestring(image_64_encode)

ADVANTAGES:

- Successfully stores look and feel of existing information.
- Effectively stores look and feel of existing information and rapidly and effectively manages huge sums ofdata.
- Masks information.
- Useful in circumstances where the information isn't required.

DISADVANTAGES:

- When managing immense measures of information as it might be too hard to even consider finding enormous amounts significant information tosubstitute.
- Ineffective when managing modest quantities of information. Since, unique information is as yet present, if the calculation utilized was not adequately refined, may be"unshuffled."
- Encryption obliterates designing just as the look and feel of the information. Thus, it is anything but difficult to see when information has been encoded where information or if nothing else arealistic estimation of the information is required by the testteams

OUTPUT :

Input string is : menon
Encoded string is : bWVub24=

PROPOSED ALGORITHM:

This area gives the nitty gritty portrayal of proposed muddling strategy called MONcryptSSA.
Information confusion is as of late prominent in the field of security in the cloud. The proposed procedure is utilized for the information insurance without loss of data content. Steps engaged with the proposed MONcrypt SSA are asfollows:

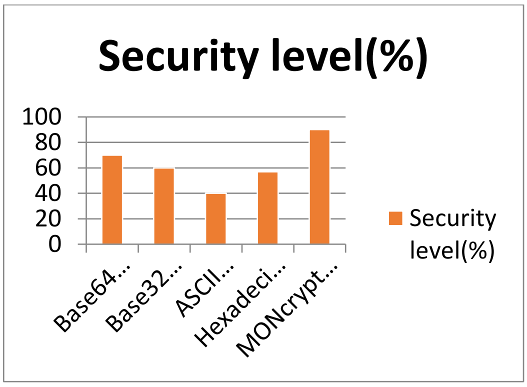
- Users present the PlainText (PT) and key (K) to MONcrypt SSA. □
- Determine the numerical qualities in the PT. MONcrypt = OK (Num), (O denotesobfuscation) □
- Find the quantity of qualities in the N=sizeof(PT) .
- Calculate the square (ST) for each incentive in the PT, ST=square(PT).
- Rotate ST at K number of times, K is augmented by 1 for each continuous incentive in the PT. Rotation_ST (RT) = RK+j (ST)j =0,1,2,…
- Calculate module (MT) for RT by 256, MT = RT%256.
- Convert the MT into ASCII code to create -ciphertext(CT).

b) MONcrypt SSA TECHNIQUE ALGORITHM:

```
1. MONcrypt_digits(PT)
2. start
3. PT-plaintext
4. N-sizeof(PT)
5. fori= 1 toN
ST(i) = pow(PT(i),2),i=0,1,2...<N
RT(i) = rotate(ST(i),K+j)
,j=0,1,2...<N MT(i) =RT(i)%256
count(i) =
MT(i)/256
CT(i)
=ascii(MT(i))
6.endfor
7. CT = cipherText

8.end
```

OUTPUT :



ADVANTAGES:

- ➢ The principle bit of leeway of MONcrypt is to decrease the information size which are put away in distributed storage.
- ➢ It changes over the numerical information onto ASCII character code. The current obscurity strategies in the writing are not decreasing the information size.
- ➢ Hackers are not capable recoup the originaldata
- ➢ MONcrypt sets aside low effort to process the information for onfuscation.
- ➢ Latency in information transfer and download is reduced.
- ➢ Low bandwidthusage.

VII. CONCLUSION

Distributed storage is progressively proficient to store the client's information. It gives practical utilization to the SMEs. SMEs don't have full foundation to keep up their information with their premises. Information re-appropriating encourages the SMEs to adequately keep up their information with distributed storage. Information redistributing has information security issues with distributed storage. The SSA is proposed, in particular, MONcrypt. MONcrypt SSAis dependent on muddling system. As indicated by the proposed strategy, the information are jumbled before they are sent to the utility stockpiling. This strategy jumbles numerical qualities. MONcrypt SSA jumbles the plaintext into ASCII character code, so the size of muddled content is reduced.The proposed procedure guarantees the security of the information, yet in addition diminishes the size of the plaintext.

Existing methods are not decreasing the information size after muddling.

The reenactment is directed with various information sizes and execution is determined dependent on the time taken for obscurity. From the outcomes acquired, it is clear that the proposed MONcrypt gives most extreme security to re-appropriated information in least time.

REFERENCES

1. Furht B. Distributed computing basics. Handbook of Cloud Computing. Springer Science, Business Media, LLC.;2010;1–17.
2. Data Obfuscation 2013.Available from: http://www.techopedia.com/definition/250 15/dataobfuscation-do
3. Robertson C. PDF obscurity - Aprimer. 2012. Accessible from: https://www.sans.org/perusing room/whitepapers/building/pdf-jumbling preliminary 34005
4. Base64 Table. 2013. Accessible from: http://en.wikipedi a.org/wiki/Base6 4
5. Josefsson. TheBase16, Base32, and Base64 information encodings.The Internet Society. 2013 Jan. Accessible from: http://tools.ietf.org/pdf/rfc4648
6. Mather T, Kumaraswamy S, Latif S. Cloud security and protection. O'Reilly Media, Inc.; 2009.

AUTHOR PROFILE

D.Samatha is a student of the Computer Science and Engineering Department at the Koneru Lakshmaiah Education Foundation situated at Vaddeswarm, Guntur District.

D.Sindhura, is a student of the Computer Science and Engineering Department at the Koneru Lakshmaiah Education Foundation situated at Vaddeswaram, Guntur District.

K.Kalpana, is a student of the Computer Science and Engineering Department at the Koneru Lakshmaiah Education Foundation situated at Vaddeswaram, Guntur District

Ms.T.Santhi Sri, working as a Asst.Professor in Computer Science and Engineering Department at the Koneru Lakshmaiah Education Foundation situated at Vaddeswaram, Guntur District