ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 12(41), DOI: 10.17485/ijst/2019/v12i41/145563, November 2019*

Reduction of Data Risk in Cloud Computing Through the Front Layer Security Mechanism

Rahul[1] and Dr. Prateek Jain[2,*]

[1]Department of CSE, Manav Rachna International Institute of Research & Studies, Faridabad 121003, India; Rahul21@gmail.com
[2]Accendere CL Educate Ltd, New Delhi 110044, India; prateek.jain@accendere.co.in

Abstract

Background/objectives: The centralised computing defines cloud computation as centralised model which is responsible to provide the network access on-request basis to a shared pool of interconnected computation resources linked together. The same is done to provision in a quick manner and to be released with the minimal management effort or cloud provider interaction. It is a platform that is built to customer convenient interface with IT framework. The promise made by the cloud computing, especially shared cloud can be decked by security infraction which are indefeasible. **Methods/statistical analysis:** An encryption and decryption algorithms have been proposed so as to maintain the security of the private data that is being transmitted in the cloud scenario. **Findings:** The increasing necessity for the secure cloud storage being handled in a centralised fashion and thereby the enticing effects of the cryptography at client side help us in prioritising and combine them together, thereby naming an innovative mechanism for the private data as third-party security and regulation issues. **Improvements/applications:** The proposed work provides a more secure framework layer as security to the data, but still there are various aspects which need to be addressed in future. Proposed work is suitable only for selected private data rather than a huge data input by user on cloud, we can extend this work for different types of modules with timestamp encryption converted time and efficiency in future. In future, the technique of Each Word Secure Authentication would be added to improve cloud security on behalf of private. Based on the security solutions, we will demonstrate a secure new client-side framework with advanced algorithm implementations in this article.

Keywords: Cloud Enhancement, EWSA, Cloud Server, Secure Cloud Platform

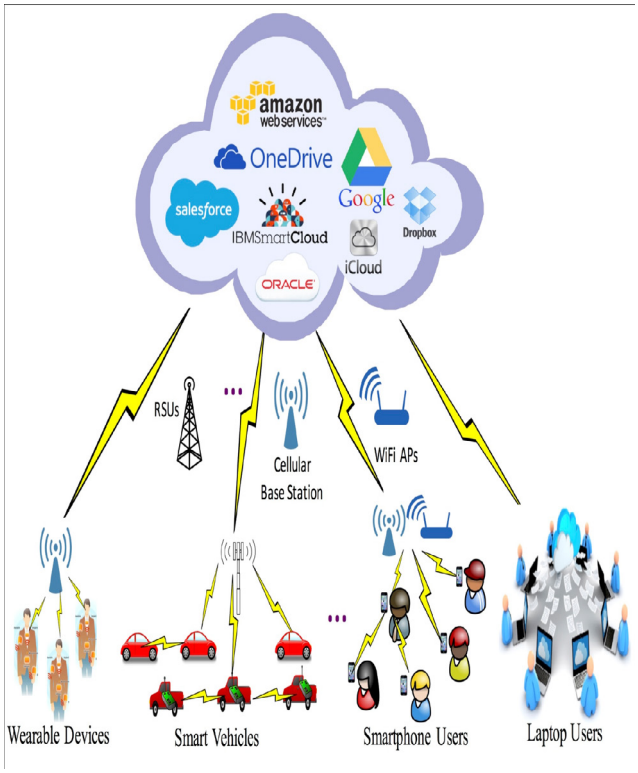
1. Introduction

Cloud computing aims at delivering the computing resources to the consumers on the demand basis or on pay as you go policy. The major advantage of using this standard computing mechanism is its low cost and the user need not to pay for the unused resources and due to this reason this technology is becoming popular among the businesses of small, medium, and large scale as well as in the government organisations. All sort of businesses are trying to utilise this technology as much as possible.

This computing mechanism is so advanced that the business managers can outsource the various tools to be used by their employees in the company and those tools and services need not to be purchased in full by the company. So the employees can access any application using this computing mechanism, including the Software's, Infrastructure as well as the hardware (Figure 1).

Cloud framework is a huge pool for centralised accessible virtualised resources services such as development services, transmission services, and internal/external components. These pools of components are composing a utilised type by go per use model.

*Author for correspondence



Cloud Computing Model

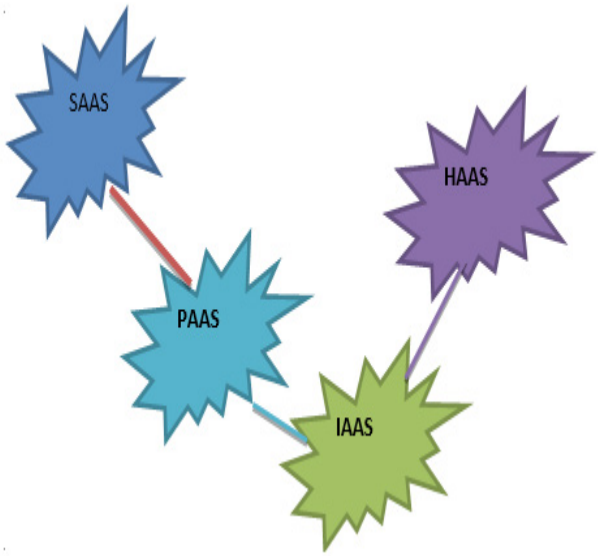
Figure 1. **Centralised sharing model of cloud computing.**

2. Services Offered by Cloud Computing

It provides the computing facility to the clients in a different manner as that to traditional computing and they are being serviced by various cloud service providers providing different sort of services. All the services that are being provided by Cloud Service Provider are based on Pay as You Usage mechanism. One Cloud Service Provider can handle n number of clients too. The services being provided by this computing technology are discussed in Figure 2.[1]

2.1. Software as a Service (SaaS)

The access to the software is being given to the user on demand only and the same is done via web browser typically. This helps the users to save the time and efforts in software deployment as well as the maintenance which tends to be very costly. The software is quite often shared by the various tenants and the same is automatically updated from the clouds as well. There is no need for purchasing the additional license to the user too. The typical example can be the Google Apps.



Cloud Computing Services

Figure 2. Services of cloud computing.

2.2. Platform as a Service (PaaS)

The aim of this service is to provide the platform for computation and also acts as stack as a service. It works by hiding all the hardware complexities and thereby providing the facilities required for supporting the complete lifecycle which is responsible in building and deploying the web-based apps and services entirely using the internet mechanism.[2]

2.3. Infrastructure as a Service (IAAS)

This service is responsible for providing the virtualised computing resources to the users over the internet. It includes providing the virtual machine access, virtual libraries, block and file based storage, firewalls, etc. The examples may include Microsoft Azure platform and Rackspace.

2.4. Hardware as a Service (HAAS)

This service is responsible to provide the hardware resources to the customers on the rent basis. Hardware can include the servers, desktops, notebooks, etc. and all these resources are given on the monthly rental basis without any upfront costing. The service provider

remotely monitors and administers the hardware on the client side based on the subscription basis.

3. Cloud Computing Risk

3.1. Security Based on Client Side

Cloud scenario includes the two things in its framework, namely front client and backend server. The security based on client side is always rejected/neglected. This security needs to be implemented by means of safety by physical medium as well as implementing the interface safety of an interface. How cloud service provider's safe physical like web browser through API interface is a major physical safety step. A client-side encryption methods and secure plug-ins is a major interface internal safety.[3]

3.2. Server-side Cloud Security

Many secure concerns are existing in server side by the cloud service provider. To prefer cloud computing, it is required to implement security measures on cloud framework to protect data and content within it. To enhance perfect factor ratio providers can go away verified system by third-party organisations or by security testers. A secure server-side layer is a major part for cloud service provider to implement regular security algorithms that are certified by verified security enhancement organisations.

There are a number of factors to implement security in server side. One of the server-side security factors are manage encryption keys with private data. Storing Key Data with information is designated to protect is alike to leave the key in the lock of the door.

3.3. Server/Client Side Cloud Security

The main discussion point in cloud computing is how we can secure private data on the client side that is purely opposite from secure the private data on the server side.

In server-side cloud security, all secure units are handled completely by the Cloud Service Provider. The service provider thereby responsible for opting some amount of secure units for preservating the private data which is stored in the cloud scenario. Cloud Service Provider usually assigns authentication techniques for encryption, digital signing the private data. These techniques are encrypted keys which are kept by service providers.

When security of data implements on client side, either the cloud user gets in charge of implementing cloud security of the private data or Programmer who provide an interface to access cloud data are responsible to implement security. Both have control over the encryption keys with encryption algorithms. They are responsible to control authorisation or access permission to private data.[4]

4. Issues Related to Cloud Computing

The secure units are examined to be a key barrier in the path goes to success. A number of researchers had already discussed a new issues research raise by CC. The security of the private data is the key concern within the cloud framework. Many cloud security issues are given below:

- ✓ **Location Transparency**
  It is the ability for cloud computing, which is occur same time during security problem, without intellect exact location of data storage.
- ✓ **Distributed Denial of Service**
  It can be a probable problem of cloud computing. In the cloud computing framework, the major attack until now and there is no option to detract such type of problem.
- ✓ **Data Protection**
  Many cloud users sharing cloud framework at any point of time. Cloud user private data is under cloud provider's control that is inputting and outputting in the shared environment. Any mean inside cloud can interfere with cloud user private data that may cause many security problems because of the lack of transparency.
- ✓ **Multi-Tenancy**
  A single cloud provider serves multiple cloud users by sharing of resources it causes some security issues like virtualisation and resource management for isolation.
- ✓ **Data Access**
  In situation an organisation can use cloud services as a third party for conducting its business process.
  Each employee of organisation considers policies to access business private data. To keep away from, break down by unauthorised access, the policies of cloud security must followed by cloud.
- ✓ **Data Confidentiality Issue**
  In the cloud computing framework, cloud users can input private data on remote servers accessible through

the internet. The data secrecy issues are raised when any government agency or any other private shares the data saved on cloud.

✓ **Data Infraction**
In cloud framework, many cloud user private data and the organisations private data are lying together. The cloud framework infracting will potentially attack the whole data of all others users.

5. Existing Work

Sidhu and Mahajan[5] presented a mechanism in this article which shows the conversion of simple text to whitened text first in the hexadecimal format. This conversion operation is performed by using the MD5 encryption algorithm which is again converted by the use of encrypting algorithm known as AES. Hence, two algorithms are being used for the encryption which includes one algorithm for the simple data and another one for the already encrypted data. The scheme presented by the authors seems quite simple and easily implementable but there is a doubt on the feasibility as there is a comprehensive usage of algorithms being done.

Kalaivani[6] implemented RSA, AES, and Steganography to provide maximum security in cloud computing. By implementing these three algorithms, authors try to provide authenticity, security, and data integrity to that data. Author tries to improve the time complexity by using other security algorithms.

Singla and Singh[7] dealt with data security issue during transmission of data. The main consideration is to encrypt private data to achieving confidentiality. Only the authorised cloud user can fetch the private data. Even if some unauthorised user gets access of the private data intentionally, he will not be able to decrypt it. This algorithm used here is Rijndael Encryption Algorithm (REA) along with EAPCHAP.

Kaur and Singh[8] represented the various encryption techniques to make the data secure on cloud. There are various encryption algorithms are explained in this article that are RSA, AES, DES and the Blowfish, etc.

Popatrao and Ansari[9] introduced a system which will prevent from the malicious resources TPA cannot be forged and also uses a better scheme of signature. It provides the feature of fine grained dynamic data update which helps in improving the efficiency of the update process as well. There is a usage of third-party auditor which can achieve the public auditing ability, stateless verification as well as the data dynamic.

On the behalf of above-mentioned factors or existing work, we are making new proposed algorithms to encrypt and decrypt private data with lines of protection program or algorithm that is "Each Word Secure Authentication" (EWSA) with "Trusted Timestamp" feature.

6. Proposed Work

Proposed model is to be presented principle of secure private data both during data transmission and data on cloud servers.[10–12] The proposed cloud interface architecture being used is as shown in Figure 3.

6.1. Proposed Algorithms with Experimental Results

6.1.1. Proposed Encryption Algorithm

Step1: Start Process

Step2: Input Private Data and save it into Variable.

Step3: On Submit Button Click, Fetch Whole Private Data from Variable to temp variable and convert it into ASCII code and save it into ASCII Variable.

Function: ["Encoding. ASCII. GetBytes.String"]

Step4: Fetch Current System Timestamp and Convert it into Milliseconds.

Function: [CurrentTime.TotalMilliSeconds]

Step5: Fetch Mid Number from Milliseconds Variable.

Function: [Start_Value + End_Value / Mid_Value], [Start_Value + End_Value / Mid_Value] +1, [Start_Value + End_Value / Mid_Value] – 1

Step6: Add Mid Milliseconds number into ASCII Variable values with word one by one after one space using foreach loop until end process.

Step7: After Add Process, Convert ASCII into plain text.

Step8: Now Transmit encrypted data into server with appending of mid millisecond variable value at the end of whole data.

Step9: Encrypted data will save into the server.

Step10: Stop Process as shown in Figure 4.

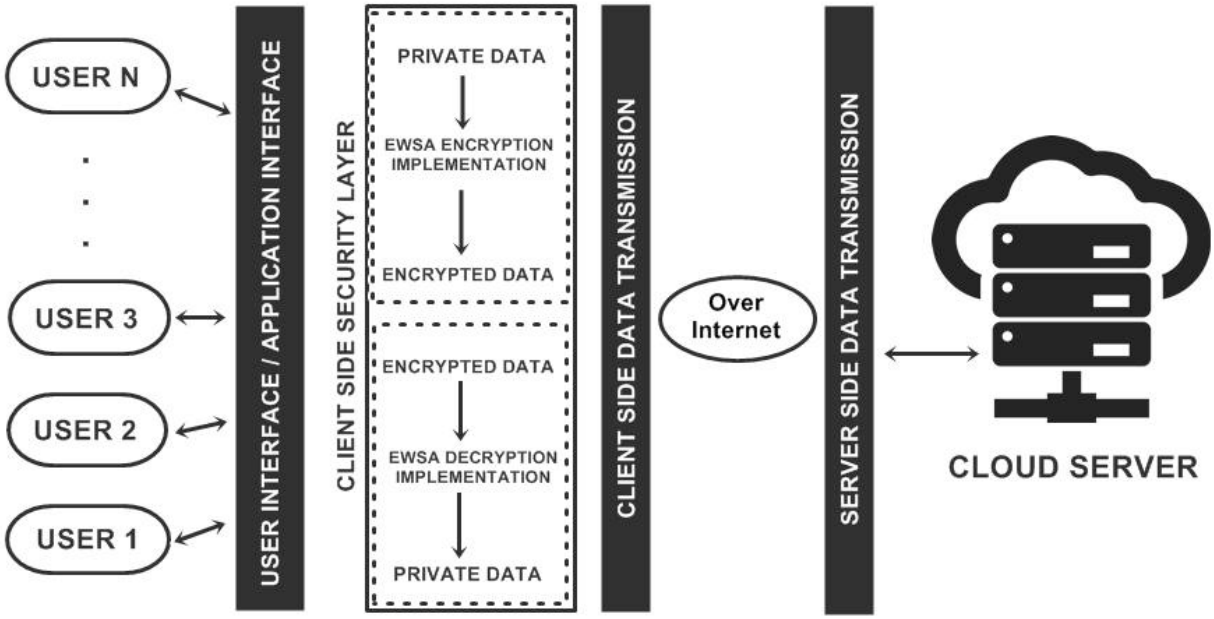


Figure 3. Cloud interface architecture model.

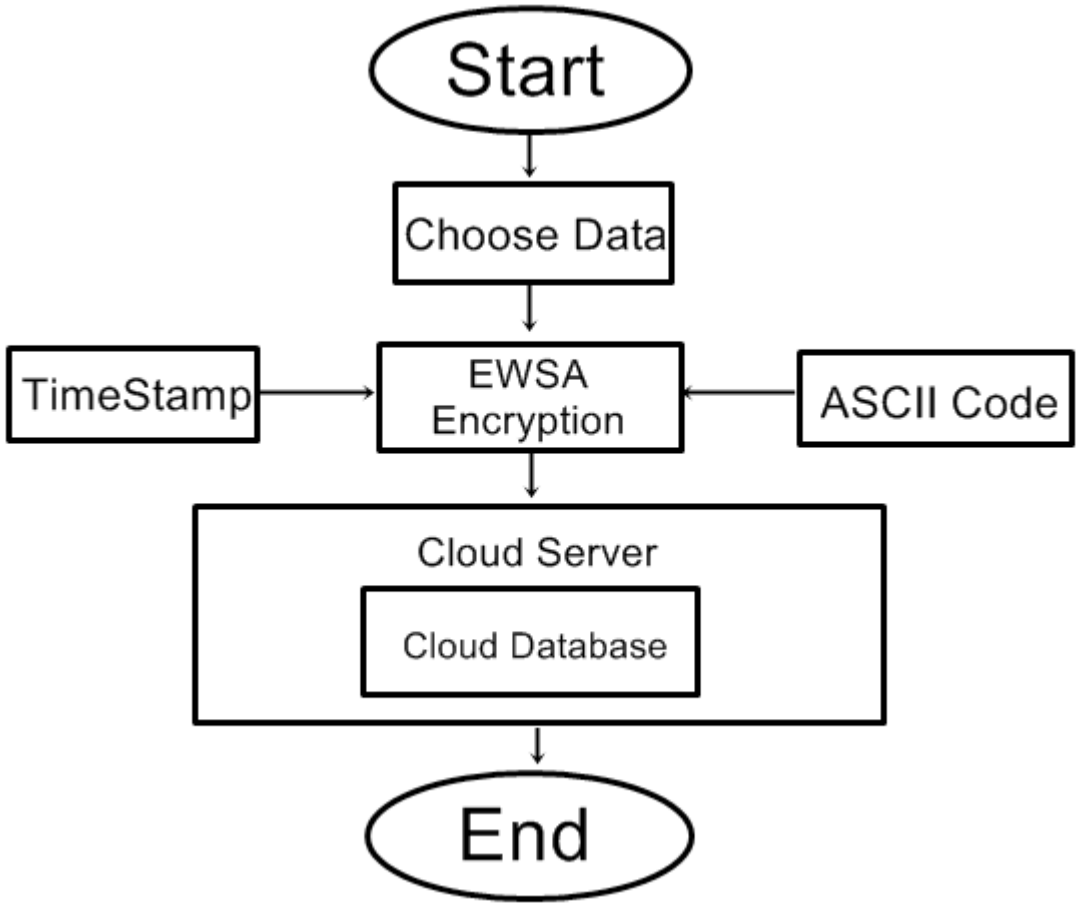


Figure 4 **Data encryption flow diagram.**

6.1.2. Proposed Decryption Algorithm

As shown in Figure 5.
Step1: Start Process

Step2: Wait For Retrieval data command.

Step3: If Retrieval command is inputting
Then Fetch Encrypted Data from Server into Variable_All.

Step4: Keep N position values into Mid_Milli_ Variable and start foreach from (N−1 to 1) untill next MergedTimeStamp indexing not fetched from Text.
If (Next MergedTimeStamp 'F' Found)
Then All text from position N−1 to F+1 copy to ASCII Variable.

Step5: Then Convert ASCII Variable value into ASCII Code.

Step6: Then Subtract N Value into All ASCII Word From Start To End until ASCII Variable string is not empty!

Step7: Then Copy this Original Data into Original_Variable.
If Variable_All is empty Go To Step8
Else Go To Step4.

Step8: Copy Original_Variable data into output screen.

Step9: Stop Process

7. Experimentation & Results

7.1. Experimentation with Cloud Computing

For experimentation with the cloud computing, the following steps are followed (Figure 6):

✓ We purchased Amazon AWS Services with Amazon EC2 Services.

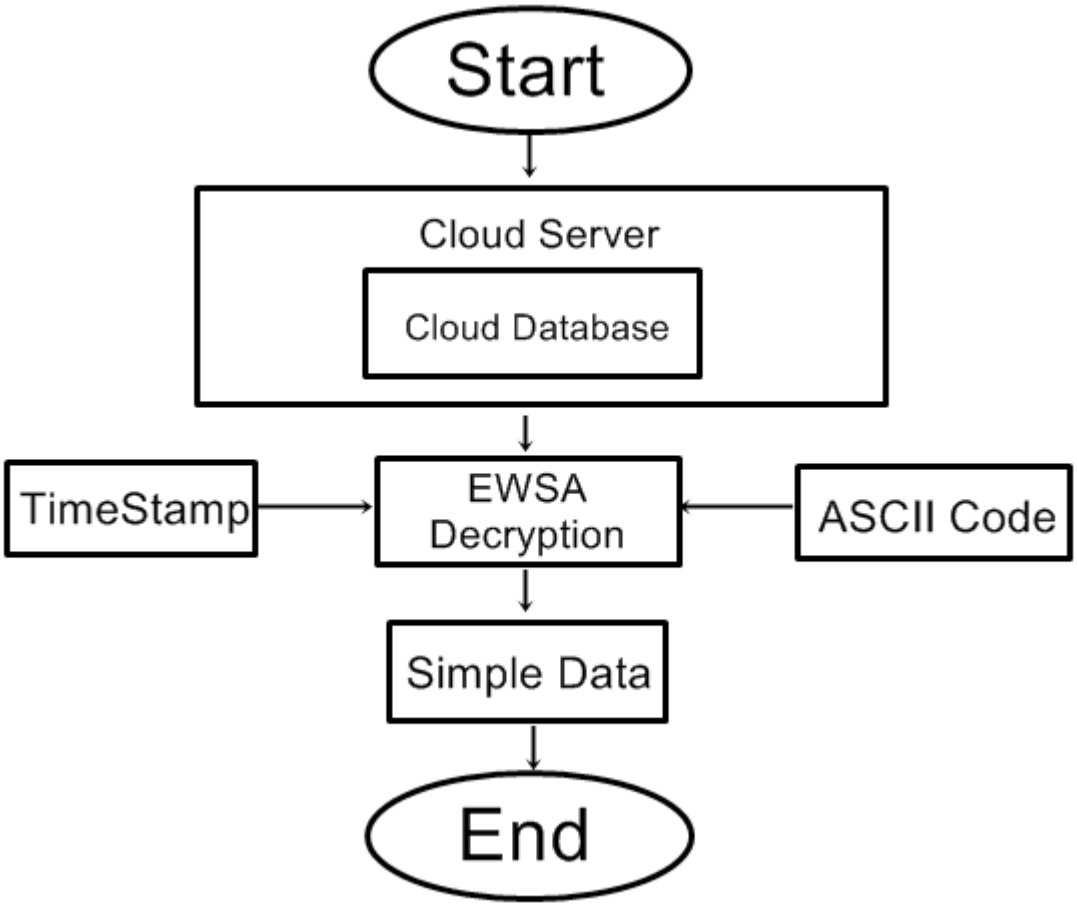


Figure 5. Data decryption flow diagram.

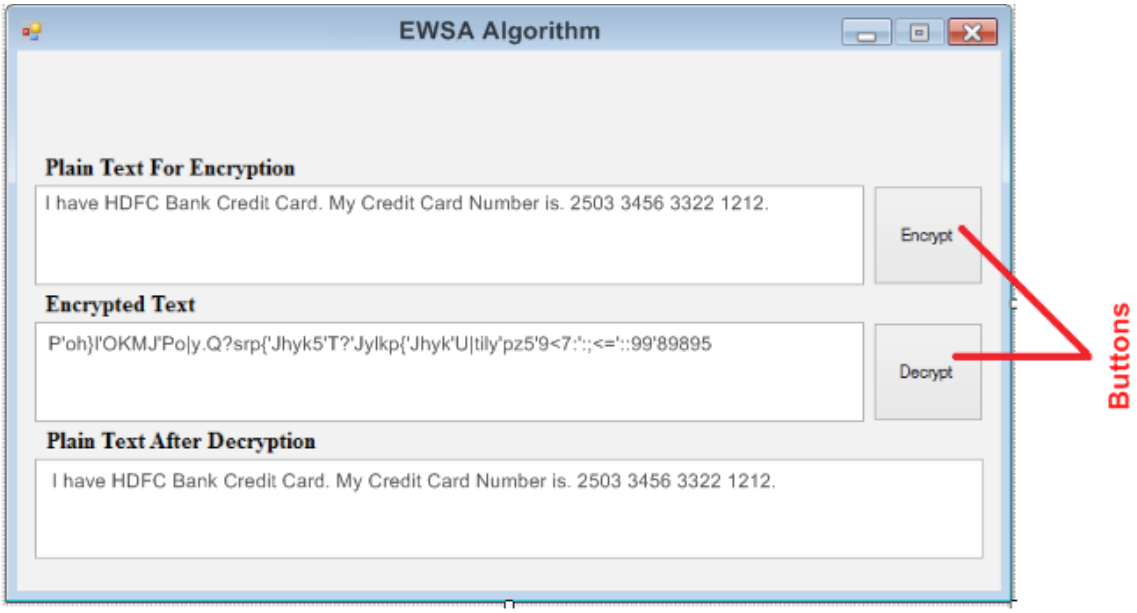


Figure 6. Experimental results of proposed work.

- ✓ They are using various security solutions like antivirus and firewall on operations for prevention of attacks on every machine.
- ✓ Then we developed android as well windows app that is done in C# language with .Net Framework with Xamarin Application Development Platform.
- ✓ In this we have used ASCII Conversation behind data we want to input on cloud server. Then we fetch Long Current Timestamp and Convert it into Milliseconds and then find mid number within milliseconds. Now we append this fetch milliseconds ASCII number with full text ASCII with Arithmetic (+) operator.
- ✓ Encrypted data are sent from web service layer to remote cloud server with index log history for Current Time.
- ✓ So when we open text direct into Amazon server for view mode as administrator point of you or as a guest, it was not in readable form.
- ✓ So through the proposed encryption mechanism we have not implemented only encryption but have also used the current timestamp model feature behind it.

Some basic parameters that are using for experimentation in platform. Experimentation done for checking the conducts of proposed cloud architecture under EWSA encryption algorithm is given (Table 1).

Test Case:

Selected Text:

Table 1. Some parameters useful for experiment

Parameter	Value
Platform	Xamarin
Programming language	C#
App nature	Android, windows
Traffic model	FTP
Architecture	Client-side security
Data Nature	Private data

I have HDFC Bank Credit Card. My Credit Card Number is. 2503 3456 3322 1212.

Converted ASCII Text:

073 032 104 097 118 101 032 072 068 070 067 032 066 097 110 107 032 067 114 101 100 105 116 032 067 097 114 100 046 032 077 121 032 067 114 101 100 105 116 032 067 097 114 100 032 078 117 109 098 101 114 032 105 115 046 032 050 053 048 051 032 051 052 053 054 032 051 051 050 050 032 049 050 049 050 046

Current Time: 25-10-2016 15:00:00

Converted Milliseconds is: [Ref: currentmillis.com]

25-10-2016 15:00:00 = 147738 7 800000 [Mid Number: 7]

Now 7 is Added using Arithmetic ADD Symbol with Selected ASCII Text Value.

Final Result:

Encrypted ASCII Text:

080 039 111 104 125 108 039 079 075 077 074 039 080 111 124 121 046 081 128 115 114 112 123 039 074 104 121 107 053 039 084 128 039 074 121 108 107 112 123 039 074 104 121 107 039 085 124 116 105 108 121 039 112 122 053 039 057 060 055 058 039 058 059 060 061 039 058 058 057 057 039 056 057 056 057 053

As from the above example, we have shown the working of our proposed encryption and decryption mechanism. We have taken the selected text as: "I have HDFC Bank Credit Card. My Credit Card Number is. 2503 3456 3322 1212" and while sending this text to the cloud server from client side this was first encrypted using our proposed encryption algorithm and we got the encrypted ASCII text. Later on we have fetched the Long Current Timestamp and Convert it into Milliseconds and then find mid number (It is 7 in our example) within milliseconds. Now we append this fetch milliseconds ASCII number with full text ASCII with Arithmetic (+) operator and thereby we got the final Encrypted ASCII text which is totally secure at the client side. Later the same process of decryption will be followed and at the receiver end user will be able to read the specified selected text properly. Thereby, we can say that the encrypted data are sent from web service layer to remote cloud server with index log history for Current Time. While we try to open the text directly onto Amazon server in view mode as administrator point of view or as a guest, it was not in readable format. Therefore, through the proposed encryption mechanism we have tried to implement the encryption algorithm but have also tried using the current timestamp model feature behind it.[13]

8. Conclusion

Cloud computing can prove to be a boon in today's work environment; hence, this article deals with data encryption algorithm implementation with current timestamp technique. The above-mentioned technique revolves around the problem of data security and with the help of encryption at client side. As per now the above-mentioned algorithm has been implemented using c# Net. Increasing necessity for centralised secure cloud storage and the tempting effects of the client-side cryptography primacy us to combine them, thus defining an innovative solution to the private data as third-party security and regulation issues. The proposed work provides more secure framework layer as security to the data, but still there are various aspects which need to be address in future. Proposed work is suitable only for selected private data rather than a huge data input by user on cloud, we can extend this work for different types of modules with timestamp encryption converted time and efficiency in future. In future, the technique of Each Word Secure Authentication would be added to improve cloud security on behalf of private.

References

1. Tsai WT, Xin Sun, Balasooriya J. Service-oriented cloud computing architecture. In: Seventh international conference on information technology; 2010. P. 684–9.
2. Sadhasivam S. Design and Implementation of an efficient two-level scheduler for cloud computing environment. In: International conference on advances in recent technologies in communication and computing; 2009.
3. Mathew A. Security and privacy issues of cloud computing; solutions and secure framework. Int J Multidiscip Res. 2012;2(4):1–5.
4. Gaur T, Divya Sharma. A secure and efficient client-side encryption scheme in cloud computing. Int J Microw Wirel Technol. 2016;6(1):23–33.
5. Sidhu A, Mahajan R. Enhancing security in cloud computing structure by hybrid encryption. Int J Recent Sci Res. 2014;5(1):128–32.
6. Kalaivani R. Triple layer security to data in cloud. Int J Comp Sci Inf Technol. 2016;7(2):783–5.
7. Singla, Sanjoli, and Jasmeet Singh. Cloud data security using authentication and encryption technique. Glob Comp Technol. 2013.
8. Kaur M, Singh H. A review of cloud computing security issues. Int J Adv Eng Technol. 2015;8(3):397.
9. Popatrao SV, Ansari MB. Cloud with third party auditor. Int J Eng Res Gen Sci. 2016;4(3):1–4.
10. Thuraisingham B. Secure data storage and retrieval in the cloud. In: 6th international conference on collaborative computing: networking, applications and work sharing; 2010.
11. Yogeswari, G., and P. Eswaran. Enhancing data security for cloud environment based on AES algorithm and steganography technique. Int J of Adv Res Trends in Eng Techno. 2016;3.
12. Pareek P. Cloud computing security from single to multi-clouds using secret sharing algorithm. Int J Adv Res Comp Eng Technol. 2013;2(12):3261–4.
13. Rahul Sharma, Dr. Prateek Jain. An impact of digitalized technologies transformation in healthcare using mobile cloud computing. Indian J Sci Technol. 2016;9(34):1–4.