iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IX **Month of publication:** September 2022

DOI: https://doi.org/10.22214/ijraset.2022.46557

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IX Sep 2022- Available at www.ijraset.com

Development of AWS based E-invoice Platform for Trading

Thejasree R[1], Thyagaraja Murthy A[2]
[1]*MTech Student,* [2]*Associate Professor, Department of Electronics and Communication, JSS Science and Technology University, Mysore, India*

Abstract: ***Global container shipping is the phenomenon of packing goods into containers and transporting them across country borders. A global container shipping trip often involves multiple carriers, third party logistics firms, and fourth party logistics firms. Based on previously agreed-upon contract pricing with the shippers, these businesses bill base service costs, unexpected service fees, and value-added service fees through freight invoices. This study introduces an AWS-based system for creating electronic invoices for carriers of goods when one or more carriers are involved in the shipment of products from a shipper's origin location to a destination location outside of the country of origin. Real-time shipment tracking data and previously agreed-upon service contract pricing between the shipper and the carrier are largely used in the preparation of an invoice for a carrier. Our solution improves the effectiveness of the e-invoicing process and reduces expenses for the shippers and carriers involved in international trade. The' main reasons for adopting AWS-based e-invoicing solutions are to decrease the frequency of invoice disputes, speed up dispute settlement, and offer real-time audits.***
Keywords: AWS S3, AES Rijndael algorithm, Shamir's secret key sharing.

I. INTRODUCTION

Import and export of goods and services between the countries is known as Global trade. This trade includes three mode of transportation i.e land, air and sea. About 50 percent of the annual capital is contributed by shipping goods through sea. But the complexity increases when there is multiple enroute between various parties involved in movement of these goods. Overall maintaining complete transparency in shipping service becomes increasingly difficult. For this reason, carriers and shipper will attempt to gather as many details as they can for the purpose of generating invoices, settling payments and handling disputes. Eventually, as each party accumulates data according to their priorities, the invoice settlement and multi-party planning will be undermined by mistrust of information. In an effort to solve the trust and transparency issues among parties, we are is implementing innovative solutions based on Amazon Web Services. This paper proposes an AWS-based e-invoicing solution that allows participants in the supply chain network to manage contracts, generate invoices, and handle disputes. A major benefit of e-invoicing is that it helps balance data and ensures precision during manual data entry. E-invoicing provides real-time tracking of invoices, and all details of transactions between companies will be accessible online. This would eliminate the need for frequent audits and surveys. And also these invoice are encrypted using AES rijndael and and the key used for AES encryption is secured using Shamir's secret sharing algorithm and is stored in AWS S3 services. AWS Simple Storage Service (Amazon S3) provides scalability, data availability, security, and performance that are unmatched in the industry. Data can be stored and retrieved from anywhere, anytime, with Amazon S3 service.

II. LITERATURE SURVEY

D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud in their paper [1] presents a performance evaluation of symmetric encryption techniques that have been chosen. The chosen algorithms were Blowfish, RC2, DES, RC6, AES, and 3DES. They came to the conclusion that Blowfish performed better than the others when the packet size was changed. Further, it was found that moving from text to another type of data, like an image, took longer with RC2, RC6, and Blowfish than with other methods. Moreover, it was discovered that 3DES still performs poorly when compared to algorithm DES.

Srinivasarao D, Sushma Rani N, Ch.Panchamukesh and S.Neelima in their paper [2] have analysed the superlative symmetric cryptographic encryption algorithm. DES, 3DES, Rinjdal, Blowfish, RC2, and RC6 are the chosen algorithms. Following Blowfish as the best practise to prevent data misuse, followed by AES and RC6. Blowfish has the best application where the code is unbreakable. The Blowfish performs best when encryption and decryption times are changed repeatedly. And finally, when it comes to data files, we discovered that Blowfish once more performs well when compared to other algorithms, with 3DES and Rinjdal coming in second and third.

©IJRASET: All Rights are Reserved

\item Akhil K.M, Praveen Kumar M and Pushpa B.R in their paper [3] has proposed AES based secure model for cloud data security. As AES encryption is employed for data transfer, it eliminates the potential that the system will occasionally become unavailable due to the arrival of large amounts of data. Since denial of access to the third party is done, possibility of intruders to mask as the third party and intrude into the network is avoided. Thus, the suggested solution offers cloud user data an effective AES-based encryption technique.

\item M. A. Al-Shabi in his paper [4] comparison between Symmetric and Asymmetric algorithms shows that Symmetric algorithms are faster than their Asymmetric counterparts.

The most dependable algorithm in terms of speed encryption, decoding, the length of the key, structure, and usability is AES, according to past studies and comparison results.

\item Yoshita Sharma, Himanshu Gupta and Sunil Kumar Khatri in their paper [5] analysed the popular secret key algorithms including DES, 3DES, AES (Rijndael), Blowfish, were implemented, and by encrypting input files with different contents and sizes, their performance was compared.

The results, which showed that the Blowfish method is the fastest, were finally presented.

\item Karthik .S and Muruganandam .A in their paper [6] presented simulation results showed that 3DES has a better performance result with ECB and CBC than other common encryption algorithms used. They have also included a performance assessment of some symmetric encryption methods in this work. The chosen algorithms are RC2, RC4, Blowfish, DES, DES3, and AES. When the key size is changed, it is evident that the battery and time consumption alter significantly.

\item Shanta and Jyoti Vashishtha in their paper [7] presents a performance evaluation of AES and DES symmetric encryption algorithms. speed, duration, and cost performance characteristics. Better results are produced by using the AES encryption/decryption algorithm in C# in Microsoft Visual Studio. The performance of the chosen AES/DES algorithms in C++ when running in VC++ does not deliver the best results in terms of the necessary keys, such as speed, time, and cost. It was discovered that the AES/DES algorithms in C++ were slower than other algorithms. Finally, the AES/DES algorithms written in C# and executed through Microsoft Visual Studio produce the best results in terms of performance, time, and cost.

\item Abha Sachdev and Mohit Bhansali in their paper [8] presented that each of the cloud providers has their own set of rules, pricing, flexibility, support and other important parameters. The encryption strategy used to secure data by rendering it unreadable to everyone is the main issue covered in this proposal. When compared to alternative algorithms, using AES for data security offers advantages of lower memory usage and faster calculation.

\item Vishal R. Pancholi and Dr. Bhadresh P. Patel in their paper [9] concluded AES encryption is the fastest method that has the flexibility and scalability and it is easily implemented.

The AES algorithm, on the other hand, uses less memory than the Blowfish algorithm. Because it uses a 128, 192, or 256-bit key, the AES algorithm has a very high security level. It demonstrates how to increase cloud computing security with secure data storage by applying defences against multiple types of attacks, including differential, square, and key assaults as well as key recovery and square attacks. As a result, the AES algorithm is a very secure encryption technique. While other symmetric algorithms have certain flaws and variances in performance and storage space, AES encryption algorithm offers minimal storage space requirements, great performance, and no vulnerabilities or restrictions.

\item Prof. S. Delfin, Rachana Sai. B, Meghana J.V, Kundana Lakshmi. Y and Sushmita Sharma in their paper [10] revealed how For the next generation of IT applications, cloud computing is a promising and developing technology, and cryptography is one of the most significant and critical skills to protect data from hackers by applying the crucial procedures of encryption and decryption. The swift solution that is adaptable and simple to use is AES encryption. While other symmetric methods have various constraints and differ in terms of storage space and performance, the AES encryption algorithm offers good performance and requires very little storage space. In comparison to alternative methods, the use of the Advanced Encryption Standard for data security offers advantages of faster calculation and less memory usage.

\item Krishnasuri Narayanam, Seep Goel, Abhishek Singh, Yedendra Shrinivasan, Shreya Chakraborty, Parameswaran Selvam, Vishnu Choudhary and Mudit Verma in their paper [11] have spoken about the necessity for blockchain-based invoicing that speeds up the resolution of disputes between shippers and carriers in international trade and enables effective invoice settlement. Additionally, they gave information about a blockchain-based system providing trusted invoice generation and open dispute resolution, as well as a description of the blockchain invoicing strategy. The system suggested in this study uses a cloud microservices architecture and Hyperledger Fabric as the underlying blockchain platform. The findings demonstrate that it is feasible to implement invoicing systems in settings with actual clients.

III. PROPOSED SYSTEM

The Proposed System is an AWS based E-invoice application, where the invoice generated is encrypted using AES rijndeal algorithm and the key used for AES encryption are secured using Shamir's secret key sharing algorithm. The main objective of this thesis is to design a web application solution for invoice and operation and also in shipment operations which can be accessible anytime, with high handling capacity, easy to use, better time saving capability, reduce operational and service expense, providing tamper proof data.. System uses tools such as "VisualStudio" and "SQL Server" to develop application.

A. Block diagram

In proposed system shown in Figure 1, first the Manufacturer will register with their details such as company name, mail ID, phone number and address, Once registration is done the Manufacturer will login with their credentials and will add the raw materials and the Supplier(s) of their choice and will send the login credentials from the registered E-mail address. The Supplier will login with the credentials and will map the raw materials and later can edit if required. The supplier has to add the service provider once the the raw materials are mapped. The Service provider should login with the credentials sent from the registered email of the Supplier. Once the order has been confirmed by the Manufacturer, the supplier has to approve the order and map the Service provider to whom he wished to give the delivery. When the order has been approved the Invoice generated are stored in AWS S3 service which are encrypted using AES and the key used for encryption are secured using Shamir's algorithm. The Service provider will update the delivery status that can be viewed by the Manufacturer. Once all the service is done the Manufacturer will be able to download the e-invoice and rate the overall experience that can be viewed by the Service provider.

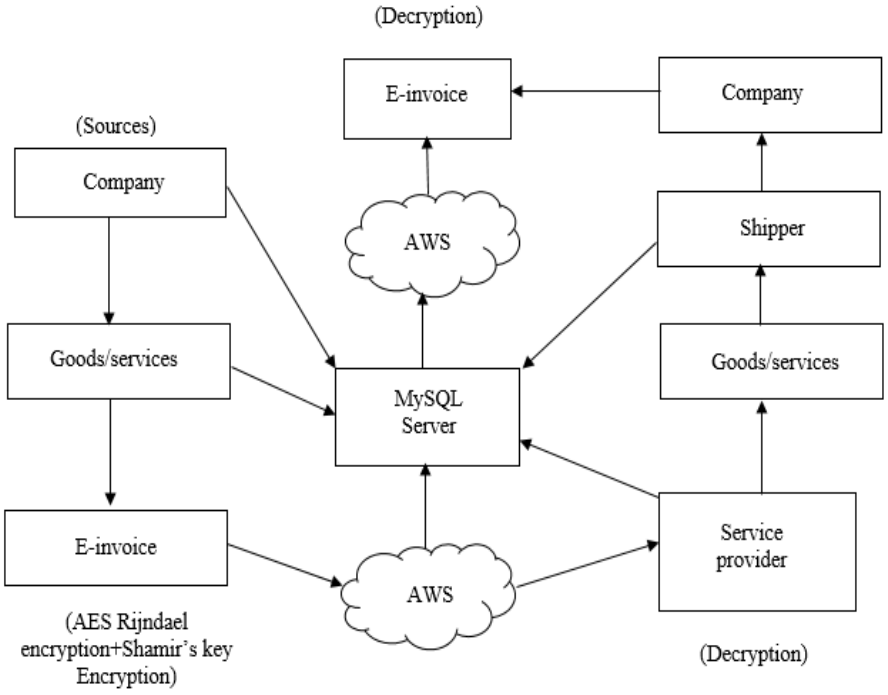


Figure 1: Block diagram

B. Module Designs

1) *Manufacturer Module Design:* In this module the company has to first register. Once the registration is successful the manufacturer will login using the credentials and will add the raw materials. Based on the raw materials added the manufacturer will add the supplier(s). Once the supplier has been added by the manufacturer, the ID and Password is sent from the registered email of the manufacturer to the supplier. Once the order is confirmed the e-invoice generated is stored in AWS cloud which are encrypted using AES rijndael encryption and the key used in AES is secured using Shamir's key sharing algorithm. Once the product or raw materials is delivered to the Manufacturer, they are able to download the e-invoice and rate the overall service. The module diagram is depicted in Figure 2. And also all the information will be stored in Sql server

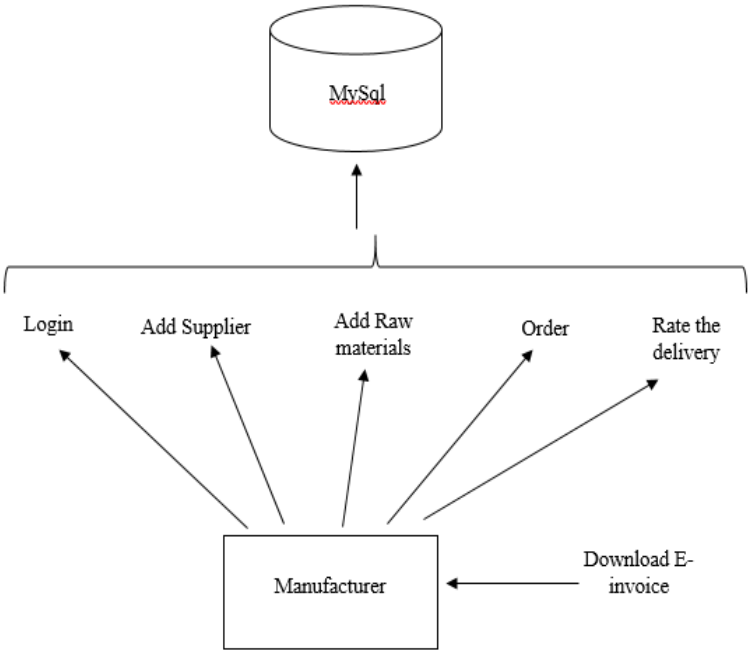


Figure 2: Manufacturer Module Design

2) *Supplier Module Design:* In this module the supplier will login based on the credentials sent by the manufacturer. Supplier can map the price of the ordered raw materials and later can view and also update the mapped raw materials. ID and password is sent from the registered email of the supplier to the service provider. And when the raw materials are added by the Manufacturer, the Supplier will add the Service provider of their choice. And finally when the order is placed and then approved by the Supplier, the Supplier will map the Service provider to whom he wish to give the service. And then the e-invoice is generated. And the e-invoice generated is encrypted using AES rijndael and the key used for encryption are secured using Shamir's algorithm and stored in AWS S3 service. The module diagram is depicted in figure 3. And all these information will stored in Sql server.

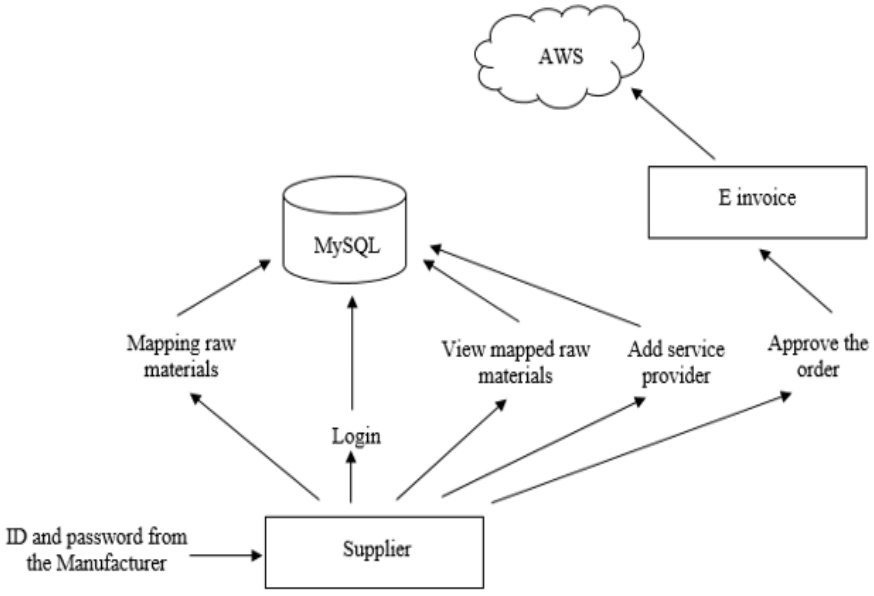


Figure 3: Supplier Module design

3) *Service Provider Module Design:* In this module the Service provider will login using the ID and password sent by the Supplier from their registered email address. And Service provider can view the service allocation and the delivery feedback posted by the company. All the information will be stored in the database. The service provider can also view the ratings given by the Company and the supplier. The module diagram is depicted in figure 4. All the information will be stored in Sql server.

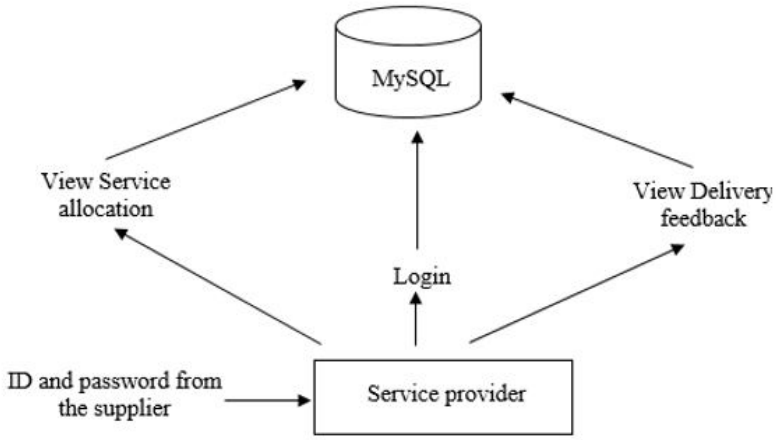


Figure 4: Service provider Module design

C. *Algorithm Implementation*

1) *AES Algorithm:* Rijndael is an Advanced Encryption Standard (AES) algorithm. Its pronunciation is rain-dahl. When it was chosen by the National Institute of Standards and Technology as the default symmetric key encryption method, it replaced the older and less effective Data Encryption Standard.

a) *AES Encryption:* The symmetric encryption technique that is most likely to be used nowadays is the Advanced Encryption Standard (AES). The AES encryption is depicted in figure 5

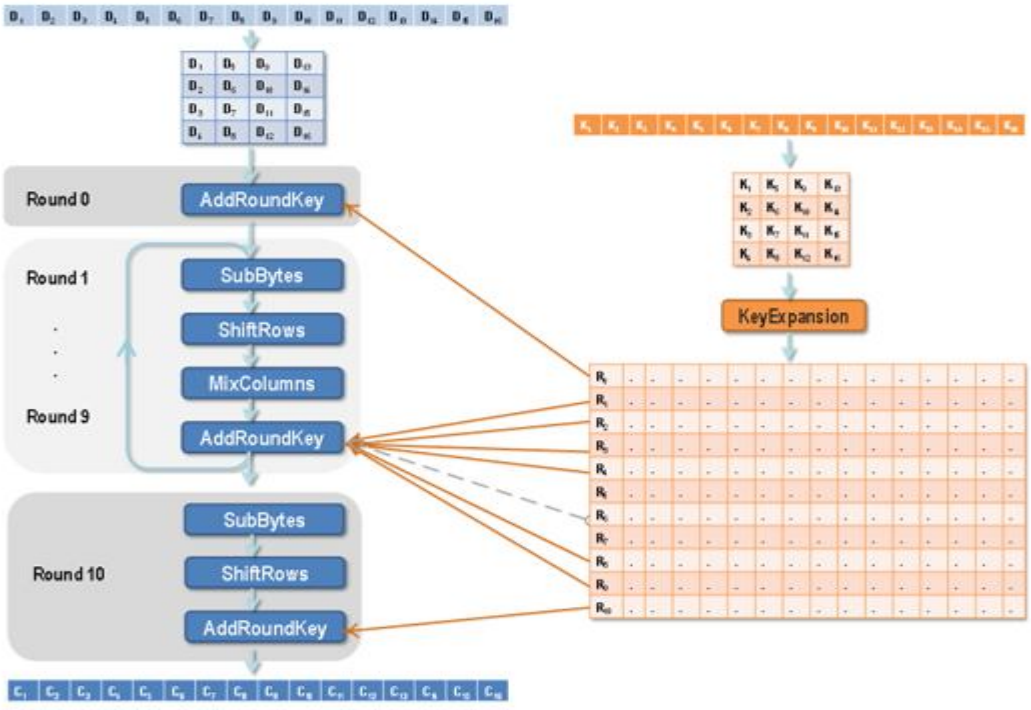


Figure 5: AES Encryption

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IX Sep 2022- Available at www.ijraset.com

➢ *Round 0*

The initial round key for AES (R0), and it is derived from the AES Key Schedule. Here each byte is combined with each byte of round key with Bitwise XOR operation

➢ *Round 1 – Round 9*

These round has four sub process

- *SubByte* – The 16 bit input is replaced according to the S-box design. The result is stored in 4X4 matrix

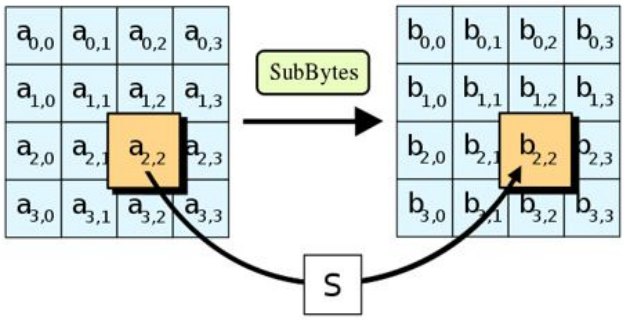


Figure 6: SubByte sub process

- *ShiftRows* – Here, the first row is left alone, but the second, third, and fourth rows are all moved one byte, two bytes, and three bytes to the left. The resulting matrix has 16 bytes, but they are displaced relative to one another.

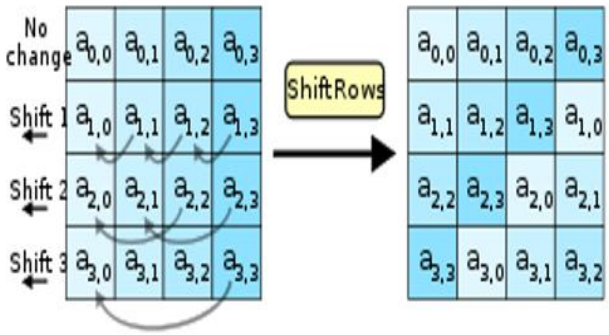


Figure 7: Shift rows sub process

➢ *MixColumns* - Here, a mathematical formula is used to change each column of four bytes. Each column's input is used to create an entirely new column of bytes that replaces the old column.

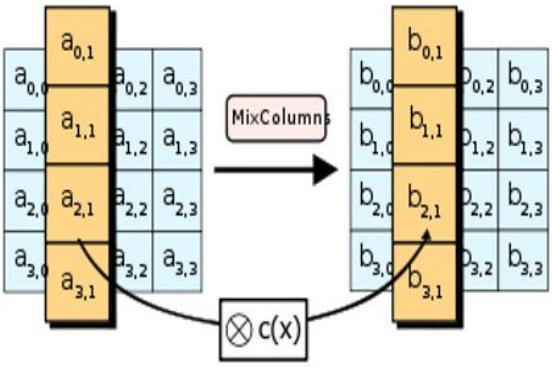


Figure 8: MixColumn sub process

©IJRASET: All Rights are Reserved

- *AddRoundKey* – Here, a round key of 128 bits is XORed with a matrix of 16 bytes, which are now thought of as 128 bits.

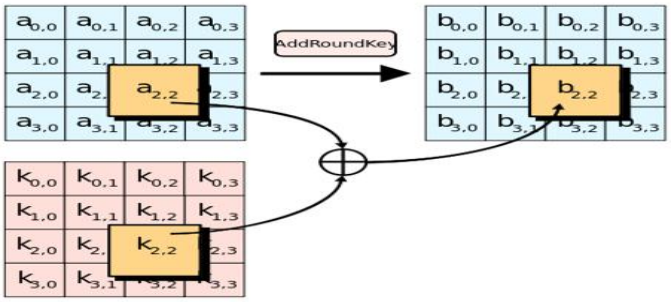


Figure 9: AddRoundKey sub process

➢ *Round 10*

This round contains the same sub process as R1-R9 except that the Mix column process is not performed. The last process AddRoundKey will generate the 128 bits Cipher text

b) AES Decryption: An AES ciphertext's decryption procedure is quite identical to its encryption procedure in reverse. The four steps are carried out in the reverse sequence in each round.

2) Shamir's secret sharing key Algorithm: Adi Shamir came up with the sharing technique known as Shamir's secret sharing in his 1979 work titled "How to Share a Secret." The secret S is divided into n pieces in this procedure so that it may be easily reconstructed from any k parts for any k < n, but the knowledge of all k – 1 pieces will also not reveal any information about S.

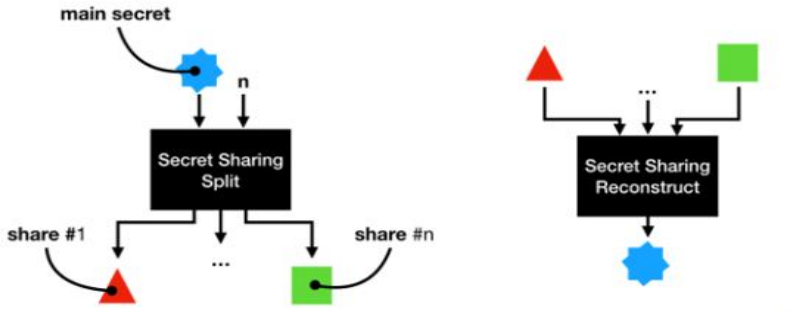


Figure 10: Shamir's secret key sharing algorithm

IV. RESULTS AND DISCUSSION

A. Homepage

When the application is opened first, it directs to start page also known as the Home page. It also acts as the content of the application. The Homepage is shown in figure 11

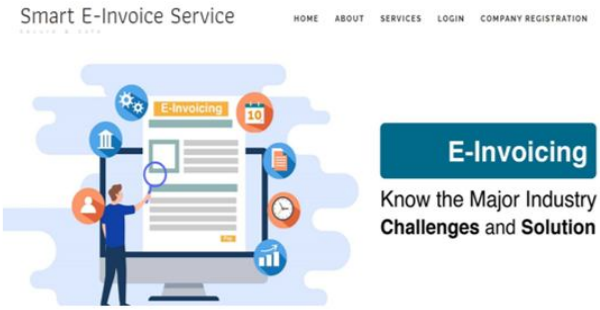


Figure 11: Homepage

B. Manufacturing Company

1) *Login and Registration Page:* The Manufacturing company should first register with their information such as company name, email ID and phone number. After register the manufacturer should login with their credentials. The result is shown in figure 12 and 13

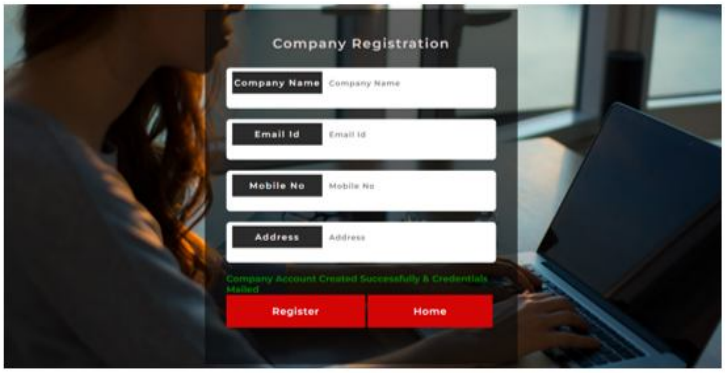


Figure 12: Registration page

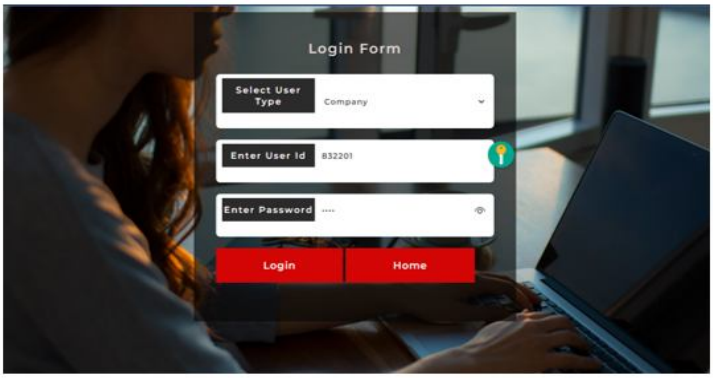


Figure 13: Login page

2) *Add raw materials and Supplier:* Once the Manufacturer has logged in with their credentials, he will be directed to the Client home page. Manufacturer can then choose to add the raw materials and the Supplier from the Dashboard options. After adding the Supplier, the ID and Password will be displayed and later the Manufacturer has to send those credentials to the respective Supplier By their registered E-mail. The corresponding results are shown in figure 14 and 15

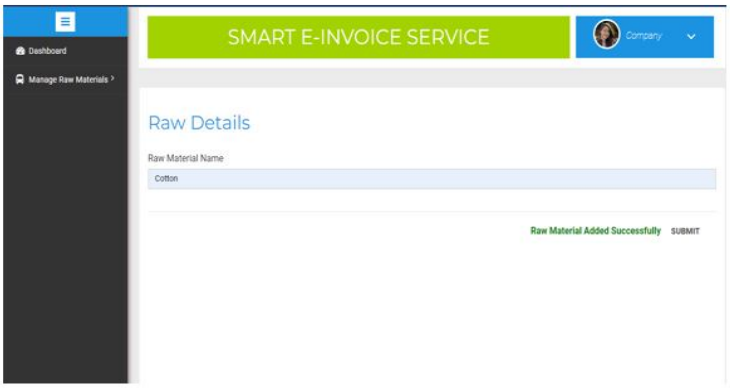


Figure 14: Adding raw materials

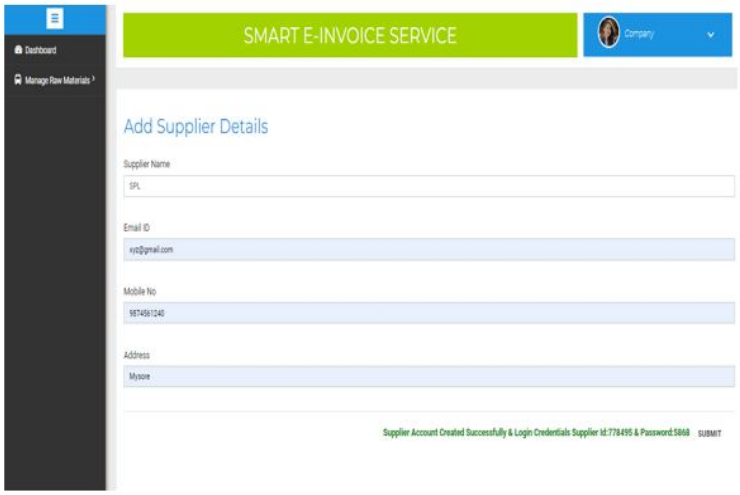


Figure 15: Adding Supplier

3) *Order Raw Materials:* Once the order is mapped by the supplier(s) the Manufacturer can then place the order to the Supplier of their choice. The result is shown in figure 16

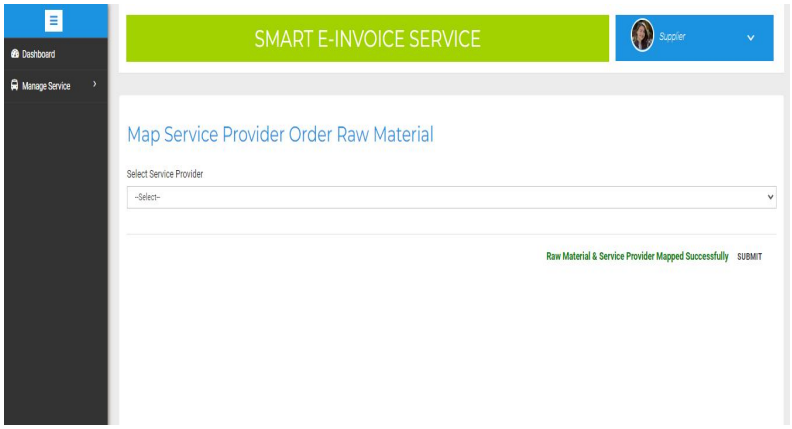


Figure 16: Order raw materials

4) *Track order, Download invoice and Delivery Ratings:* Once the order is confirmed by the Supplier, the Manufacturer can track the order, download the invoice and they can rate delivery based on the overall experience. The result is shown in figure 17

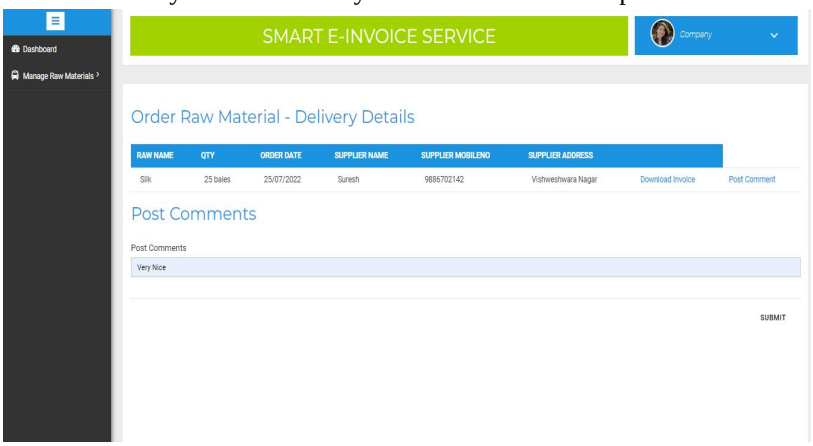


Figure 17: Track Order, Download invoice and Rate the Delivery

C. Supplier

1) Login Page: The supplier will login with the credentials sent by the Manufacturer from the registered E-mail address. The result is shown in figure 18

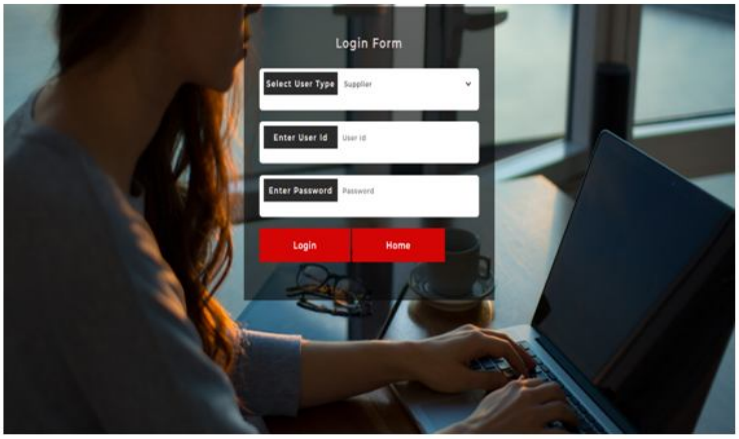


Figure 18: Login page

2) Mapping Raw Materials: Once the Manufacturer places the order of raw materials, the supplier will map those raw materials according to their price and can later view or edit the mapped materials if required. The result is shown in figure 19 and 20

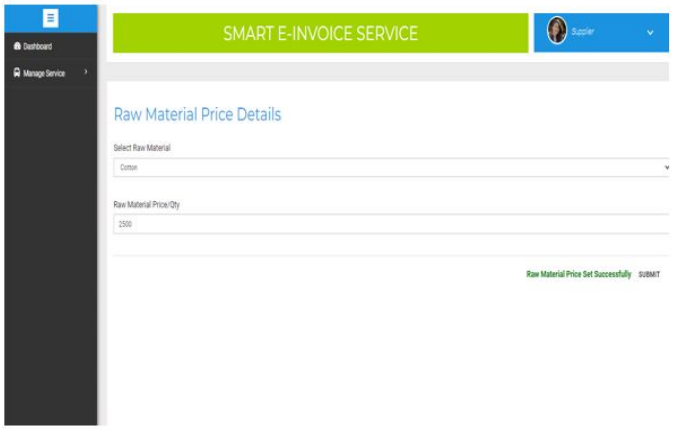


Figure 19: Mapping raw materials

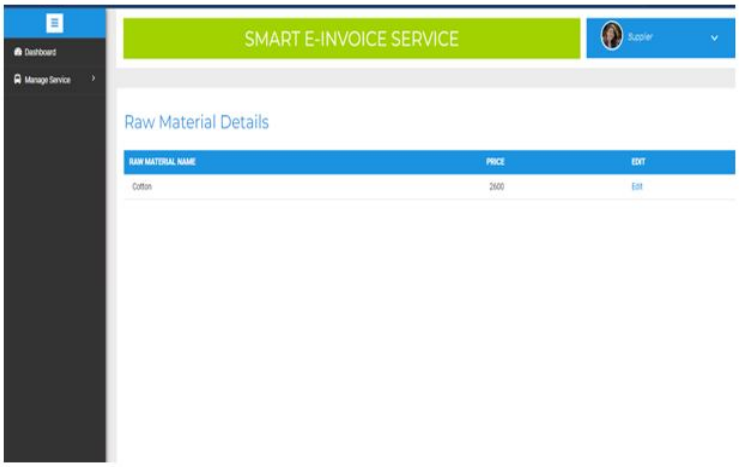


Figure 20: View or edit Mapped Raw materials

3) *Adding Service Provider:* The Supplier will add the Service provider of their choice. And credentials will be displayed which will be sent to the Service provider from their registered E-mail. The result is shown in figure 21

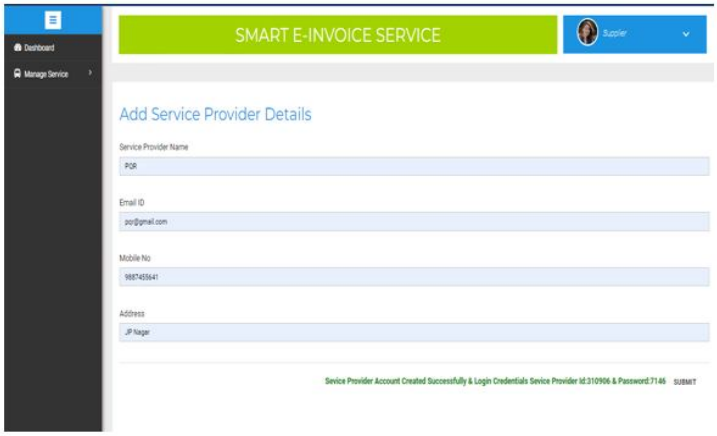


Figure 21: Adding Service provider

4) *Approving the Order and Map Service Provider:* Once the order is confirmed by the Manufacturer, the Supplier will approve the order which will be stored in AWS S3 service. Once the order is confirmed by the Manufacturer, the Supplier has to map the Service provider, who should deliver the the raw materials to the manufacturer. Later the materials will be dispatched by the service provider. The result is shown in below figure 22 and 23

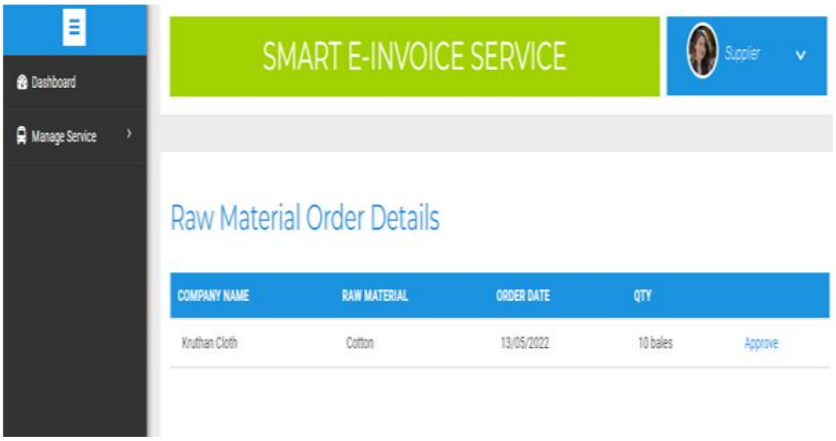


Figure 22: Approving the order placed by the Manufacturer

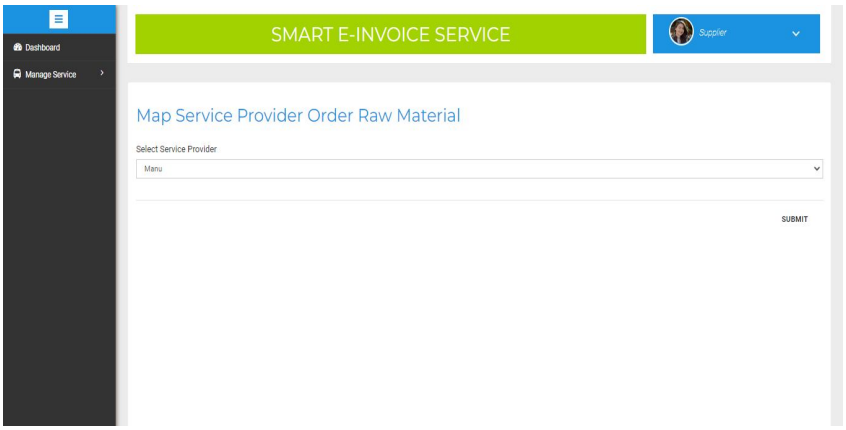


Figure 23: Mapping Service provider

5) *Creation of AWS S3 Bucket:* After approving the order placed by the Manufacturer, the AWS S3 bucket will be created were the invoivce will be encrypted and stored. The result is shown in figure 24

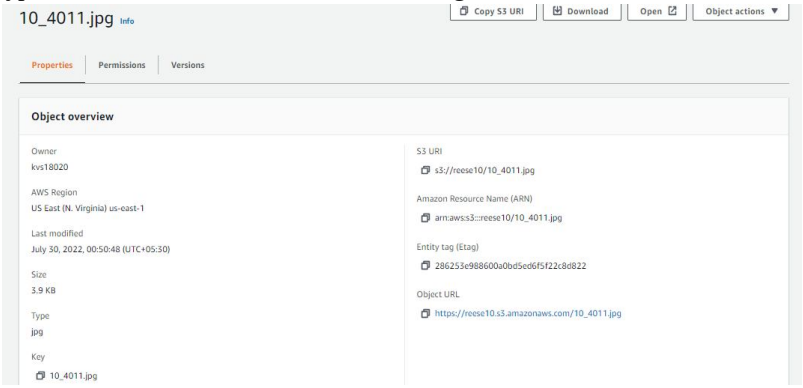


Figure 24: AWS S3 Bucket creation

6) *Service Ratings}:* Once the order has been delivered to the Manufacturer, Manufacturer will rate the overall experience of the Supplier. The result is shown in figure 25

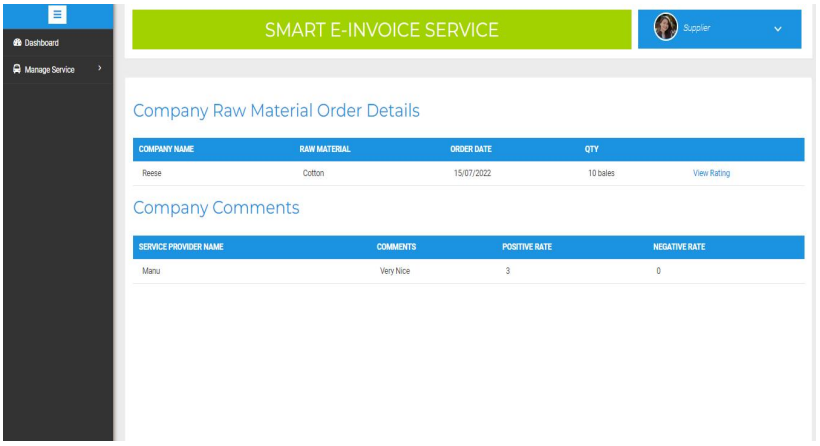


Figure 25: Service rating

D. Service Provider

1) *Login Page:* The service provider will login with the credentials sent by the Supplier from the registered E-mail address. The result is shown in figure 26

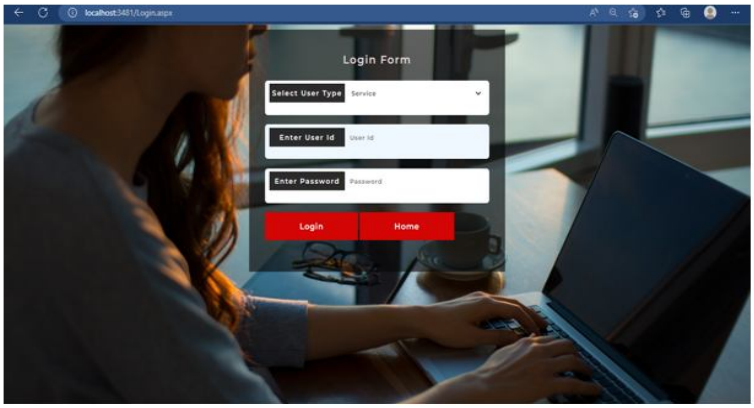


Figure 26: Login page

2) *Supplier Order:* Once the Order is approved by the Supplier, The Service provider can view the Supplier and Dispatched order. The result is shown is figure 27 and 28

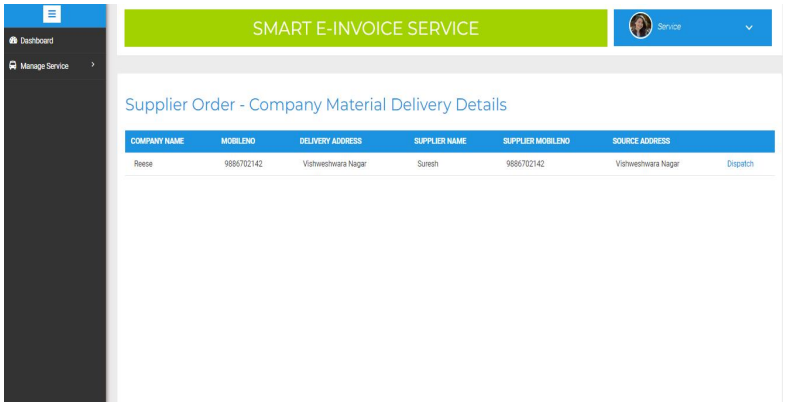


Figure 27: Supplier order

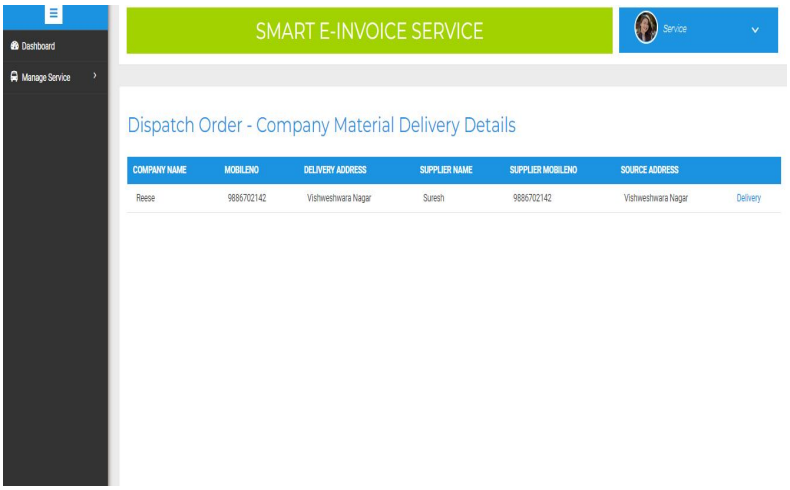


Figure 28: Dispatch order

3) *View Delivery Ratings:* Once the order is received by the Manufacturer, the ratings from the Manufacturer can be viewed by the Service provider, The result is shown in figure 29

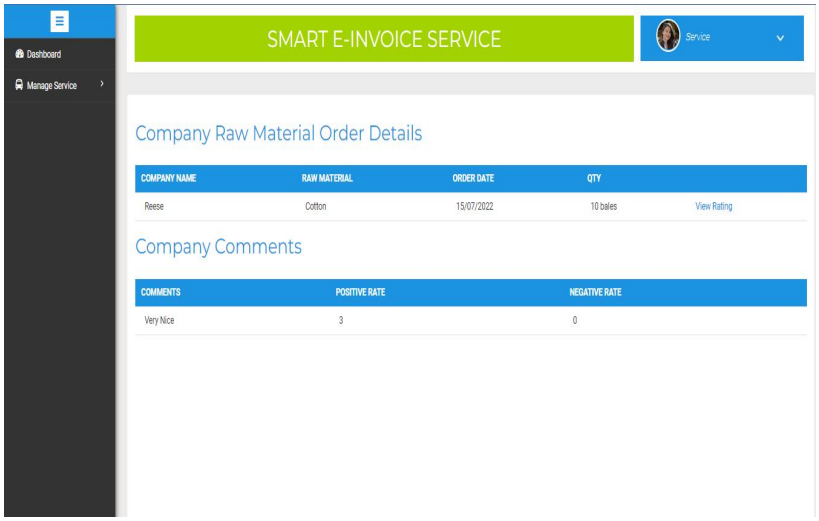


Figure 29: View delivery ratings

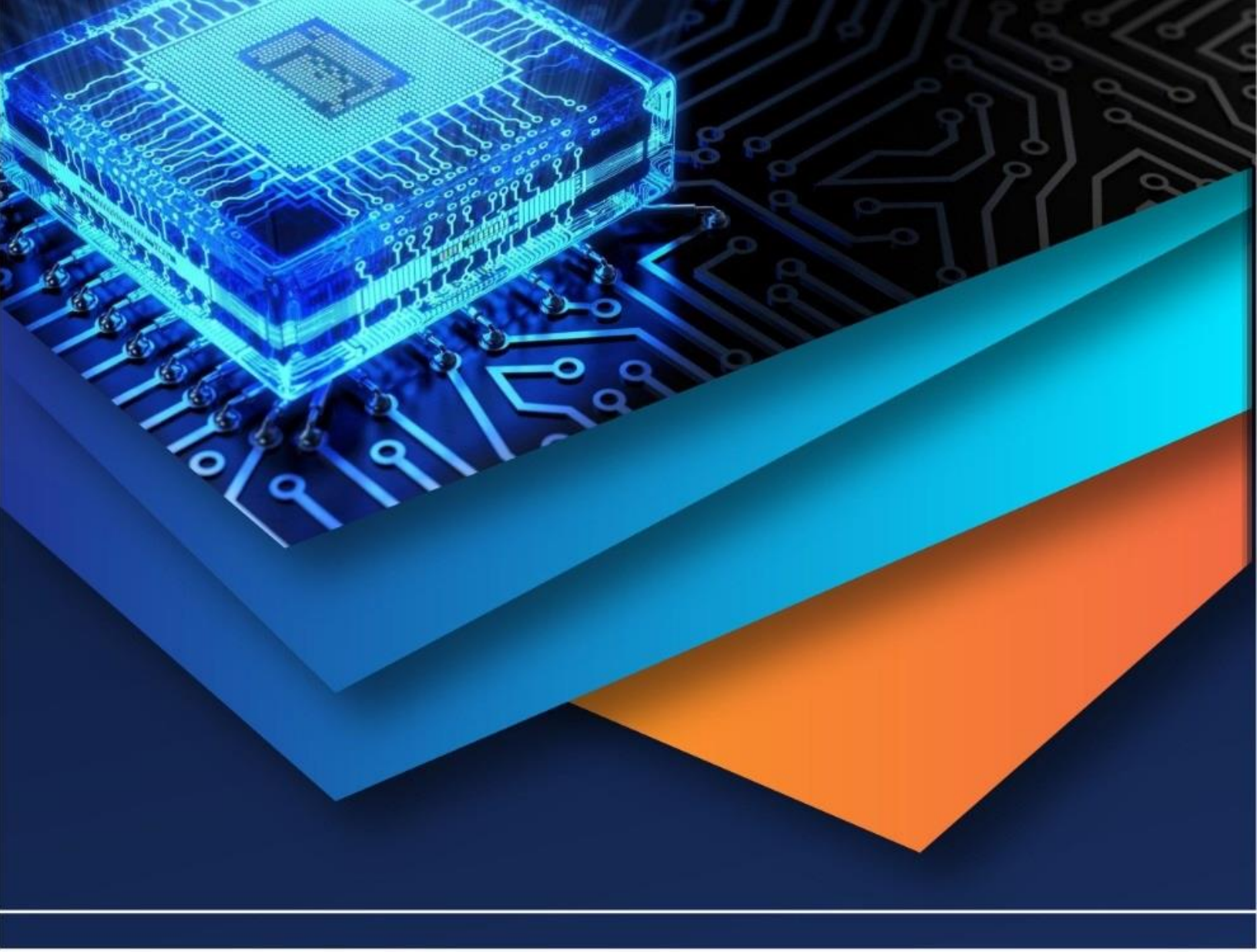
V. CONCLUSION AND FUTURE WORK

We discussed the need for an AWS-based electronic invoicing system in this article. This system would speed up invoice settlement and shorten the time it takes to settle disputes between shippers and carriers in international trade. We offered information on an AWS-based system that supports trusted invoice generation and open dispute resolution as well as our AES encrypted invoicing strategy. This article explains a series of models that serve as representations of the overall shipping processes, including Manufacturer, Supplier, and Service Provider. Contrary to traditional or self-billing invoicing processes, where invoices are often reconciled after payment settlement, the reconciliation process is carried out on the invoices before settlement of the payment. We implemented the system suggested in this work utilising the AES Rijndael algorithm, with Shamir's secure key sharing technique serving as the foundational AWS platform and S3 service. We have demonstrated that the programme offers security since the generated electronic invoices are encrypted with the AES and Shamir algorithms and because it eliminates the need for human invoice entry. Future enhancement may include implementing the intent level authorization and intent level privacy and also improving the conversational data encryption, also provide multi-factor authentication.

REFERENCES

[1] D. S. Abdul. Elminaam, H. M. Abdul Kader, and M. M. Hadhoud. “Performance Evaluation of Symmetric Encryption Algorithms”, Communications of the IBIMA Volume 8, 2009 ISSN: 1943-7765
[2] Srinivasarao D,Sushma Rani N, Ch.Panchamukesh and S.Neelima, “ Analyzing The Superlative Symmetric Cryptographic Encryption Algorithm (ASCEA)”, Volume 2, No. 7, July 2011 Journal of Global Research in Computer Science
[3] Akhil K.M, Praveen Kumar M and Pushpa B.R , “Enhanced Cloud Data Security Using AES Algorithm”, 2017 International Conference on Intelligent Computing and Control (I2C2)
[4] M. A. Al-Shabi, “ A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security”, International Journal of Scientific and Research Publications, Volume 9, Issue 3, March 2019,ISSN 2250-3153
[5] Yoshita Sharma, Himanshu Gupta and Sunil Kumar Khatri3, ”A Security Model for the Enhancement of Data Privacy in Cloud Computing ”, ISSN 978-1-5386-9346 September 2019 IEEE
[6] Karthik .S and Muruganandam .A, ”Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System” ,International Journal of Scientific Engineering and Research (IJSER),ISSN (Online): 2347-3878, Volume 2 Issue 11, November 2014
[7] Shanta and Jyoti Vashishtha, ”Evaluating the performance of Symmetric Key Algorithms: AES (Advanced Encryption Standard) and DES (Data Encryption Standard)”, IJCEM International Journal of Computational Engineering Management, Vol. 15 Issue 4, July 2012 ISSN (Online): 2230-7893
[8] Abha Sachdev and Mohit Bhansali, ”Enhancing Cloud Computing Security using AES Algorithm”, International Journal of Computer Applications (0975 – 8887), Volume 67– No.9, April 2013
[9] Vishal R. Pancholi and Dr. Bhadresh P. Patel, ”Enhancement of Cloud Computing Security with Secure Data Storage using AES”, IJIRST–International Journal for Innovative Research in Science Technology, Volume 2, Issue 09, February 2016, ISSN (online): 2349-6010
[10] Prof. S. Delfin, Rachana Sai. B, Meghana J.V, Kundana Lakshmi. Y and Sushmita Sharma, ”Cloud Data Security Using AES Algorithm”, International Research Journal of Engineering and Technology (IRJET), e-ISSN: 2395-0056, Volume: 05, Issue: 10, Oct 2018
[11] Krishnasuri Narayanam, Seep Goel, Abhishek Singh, Yedendra Shrinivasan, Shreya Chakraborty, Parameswaran Selvam, Vishnu Choudhary and Mudit Verma, ”Blockchain Based e-Invoicing Platform for Global Trade”, 2020 IEEE International Conference on Blockchain (Blockchain).

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)