Original Article

Enhanced Security in Supply Chain Management System Using AES and Md5 Algorithms

S. Raja Mohamed[1], N. Rajendran[2], I. Sathik Ali [3], M. Kabeer[4]

[1]II M.Tech Student, Department of Information Technology, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai.
E-mail: mohamedraja2098@gmail.com

[2]Assistant Professor (Sr.Gr.), Department of Information Technology, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai.
E-mail: nrajendran@crescent.education

[3]Professor and Head, Department of Information Technology, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai.
E-mail: isathikali@crescent.education

[4]Associate Professor, Department of Information Technology, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai.
E-mail: kabeer@crescent.education

Abstract

A supply chain is an order of activities engaged which circulates, assembles and handles the products to move the benefits from a dealer under the control of the last customer. It is an interconnected compound network controlled by supply and demand. Cyber security in SCM is one of the segment of its estimates of protection which primarily gives attention in managing the essential virtual protection which comprises of system software of information technology. In the existing system, cloud services must need extra applications and assistances to locate, govern and protect data which initiate extra supply chain contributors. The manufacturing process data will mislead the manufacturing process in this system based on errors which are done manually. To Store and Maintain data in a protected manner, most algorithms such as DES (Data Encryption Standard) algorithm has disadvantages and threats which seems to be an upper hand for the hackers who are working to steal the data all around. In this paper, for securing the private and secret data, we applied and executed AES (Advanced Encryption Standard) algorithm and MD5 (Message-Digest algorithm 5) in supply chain management. We apply PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyzes) approach in domain of supply chain management, data security, and cyber security to screen the various methods and algorithms which are published in various journal papers and to select a unique and best approach to be used in supply chain management and its security. This method is basically a kind of literature survey to select a best topic for doing a project or a research paper.

Keywords: Supply Chain, Cyber Security, MD5, AES, PRISMA.

DOI: 10.47750/pnr.2022.13.S03.014

Introduction

Supply Chain Management (SCM) is the major control of the progression of products and its management. It includes the growth and expansion of size of natural substances, progressing stocks, and completes the products from starting place to point of discharge. Network protection when applied in supply chain management is one of a part of its estimates of safeness which primarily gives attention in managing the required cyber security which incorporates system of information technology. Supply chain executives are easily vulnerable to digital illegal threats, malware and information thefts. There have been many occasions in which organizations were attacked through less protected points in their stock chains.

In view of this, the specific research questions are as follows.1. How research is concentrated on storing and maintaining data in SCM in a protected manner in the past few years? 2. What answers or clarifications are emerging in order to secure the organizations from hackers in supply chain.?

For answering these queries which are raised in the research, this work lead a structured analysis of the already available articles (through PRISMA). This analysis gives a way to researchers to defend about the difficulties of doing a research and give reasonable suggestions for future research (Jamaluddin and Saibani [1]). In this paper, along with making systematic review using PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyzes), we have implemented the SCM system using AES (Advanced Encryption Standard) 128-bit key algorithm and MD5 algorithm in real time to protect the data.

Literature Review

The present study aims to find the current status of cyber security and data security in SCM systems in a systematic manner by examining the literature for the past decade (2012-2021). Literature Data were collected by PRISMA approach.

Meng et al. [2] presented a review regarding the junction of Intrusion Detection Systems and block chain. In circumstances such as threats for the systems, the tools which are presented by Fraile et al. [3] give alternative protective measures for reducing the threats.

Bodkhe et al. [4] has given a structured analysis of many blockchain-based results and their application in numerous Industry 4.0-established applications. Smart contracts along with their algorithms to show interaction of entities in the system is given by Shahid et al. [5]. Gupta et al. [6] analysed the common features of AM (Additive Manufacturing) supply chain and presented three versions of AM supply chain depends on the particular type of the industry. Cydon which is a dispersed data management programme implements customised applications by using an innovative search and fetch algorithm controlling a set of data features is presented by Epiphaniou et al. [7].

Cha et al. [8] suggested a structure which uses blockchain and key escrow encryption system in a proposal to maximise the protection of Supply chain for long lasting networks and give measures for betterment of utilities for world-wide business survival. A broad analysis of 111 research papers published for open access and efficiency of Distributed Ledger Technologies in SCM is given by Asante et al. [9]. It functions as a path for present and future analysts who concentrate on SCM in view of security for good understanding of the incorporation of digital technologies such as Distributed Ledger Technologies. Mullet et al [10] have provided the technical solution which varies from traditional network protection measures to new ones, which are in relation with honeypots, etc., Pal et al. [11] provided a demanding common hypothesis to obtain constraints on heavy-tailed network protection distributions. Ahmed Khan et al. [12] suggested a unified literature based well organised detection version which is known as Deep Federated Defence Framework for Protecting Supply Chain 4.0, to aggressively spot interventions from Supply chain networks of IoT-driven CPSs using distributed local data training.

PRISMA

PRISMA method is used for fetching many existing research work to analyze and for abstracting and analyzing data, as it serves to the IEEE Xplore. The contents in IEEE Xplore comprises of more than 250 journals, more than 3 million conference papers, higher than 6,000 books and approximately 30,000 new documents are added to IEEE Xplore each month.

Four phases are there in this structured analysis which are identification, screening, eligibility, and included. In identification phase, we have searched in IEEE Xplore database, 80 papers were found in the abstracts, title of papers or keywords while searching with the keys, “supply chain management”, “cyber security”, and “data security”. This searching of papers is done in between 2012 to 2021.The searched words coincide with 80 articles from IEEE Xplore and from that 60 Conference papers and 1 magazine paper were eliminated in the identification stage. After that, 19 journal papers alone were passed through for Screening, and in that 7 papers focus on SCM security in view of physical systems and 1 paper is a corrected version of an already screened paper (might also be considered as duplicate) and so those 8 papers were further removed from the Screening stage and finally 11 are included in our Literature Review. We have given Literature review of these 11 papers in section 2. Based on the 11 studies examined, we observe that implementing SCM using AES was not seeking much attention by the researchers which lead us to implement the same. Fig. 1. shows the PRISMA methodology.

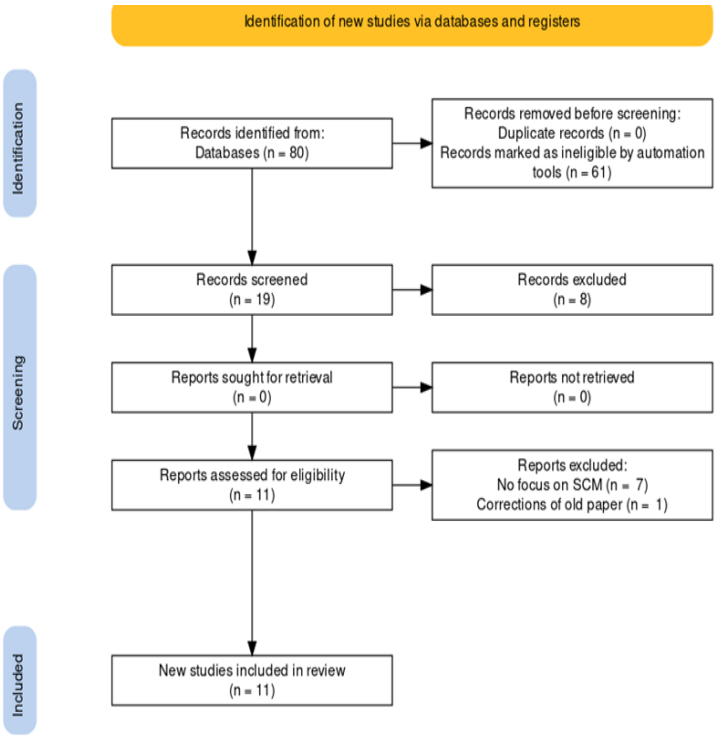

Fig. 1: PRISMA Methodology

PROPOSED SYSTEM

Any organization plans to produce some end products using the raw materials they have. For instance, multinational software companies always produce some electronic gadgets like smart phones, pc, laptops, etc., which was ordered by customers at some specific intervals of time. So, they need an estimated output of number of end products to be produced from a given set of raw materials.

In this paper, we have modelled this kind of situation where there are five components such as organization, supplier, manufacturer, distributor, customer in the order. We have made an action of sending orders from customers to organization and it is a cycle of flow of data. Organization uses AES 128-bit key algorithm and MD5 algorithm to encrypt the data of various raw materials for the purpose of securing the data from various hackers as there may be chance in more

danger of being vulnerable to cyber threats which put the organization in trouble. Here we have used MD5 algorithm in addition with AES algorithm for improving security. Nowadays many hackers easily crack various encrypted data if encrypted in a known algorithm and so we have used AES algorithm and MD5 algorithm.

It is coded in such a way that, we assign our own key instead of default key at the last stage of the algorithm. After that, organization directs the suppliers to proceed for the production of products from raw materials. Then, suppliers give the job to manufacturers to successfully produce and update the products data. Finally, distributors with the decrypted data opens the sale of end products along with their data to customers. Then after the work is over, again customers start to send orders to the organization for getting end products. The steps of architecture and the flow diagram are given in Fig.2. and Fig.3. respectively.

Steps in Architecture:

1. Customers place the orders of products to the organization.
2. This information is stored to the system before encryption using AES and MD5 Encryption.
3. Supplier decrypts this information using some keys then get the material and send it to the manufacturing department.
4. Manufacturer produces the product in organization decided manner, then update the producing information to the system.
5. The supplier is to check this information and pass it to the organization.
6. Distributor distributes the products and report selling information to the system.
7. All the system information is checked by the admin (Organization).
8. After distributing the product to the customer, again customer sends the order to the organization and this cycle continues.

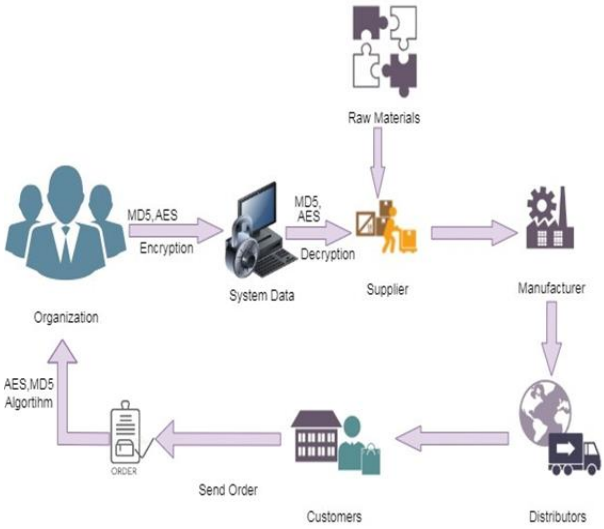

Fig. 2: System Architecture

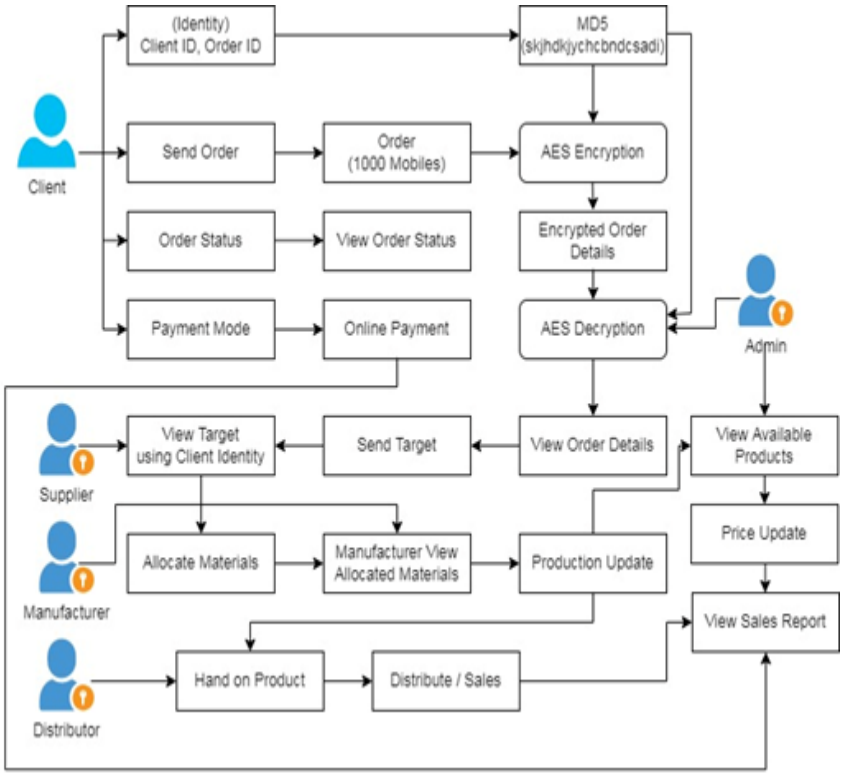

Fig. 3: System Flow diagram

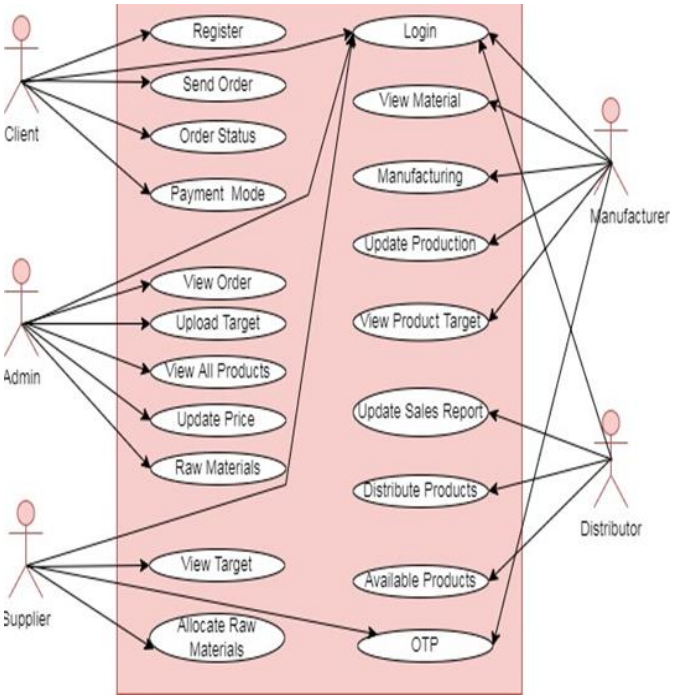

Fig. 4: Use case diagram of the system

AES Encryption Algorithm

The Advanced Encryption Standard uses the method of removing duplicate account and database processing will maintain uprightness in data and support us to validate users. It is proved that in any case, AES is 6 times faster than Data Encryption Standard. The advantage of AES when compared to DES is blocks of the text are separated into 2 equal parts but in AES the whole blocks of the text are taken into encryption to get the cipher text. (Harikrishnan et.al.[13]).

Stage 1: Called SubBytes for byte-by-byte replacement during the forward cycle. The relating replacement step utilized during unscrambling is called InvSubBytes.

• This progression comprises of utilizing a 16 × 16 query matrix to discover a trade byte for an existing byte in the info stage exhibit.

• The passages in the query matrix are made by utilizing the ideas of reciprocals in Galois field (128) and bit disarranging to demolish the bit size relationships inside every byte.

Stage 2: Called ShiftRows for moving the columns of the state exhibit during the forward cycle. The comparing change during unscrambling is meant InvShiftRows for Inverse Shift-Row Transformation.

• The objective of this change is to scramble the byte request inside each 128-piece block.

Stage 3: Called MixColumns for stirring up of the bytes in every segment independently during the forward cycle. The relating change during decoding is meant InvMixColumns and represents backwards blend section change. The objective is here is to additionally scramble up the 128-piece input block.

• The move lines step alongside the blend section step causes each piece of the ciphertext to rely upon all of the plaintext after 10 rounds of preparing.

Stage 4: Called AddRoundKey for summing up the round key to the yield of the past advance during the onward cycle. The relating stage during unscrambling is InvAddRoundKey for reverse include round key change.

MD5 Algorithm

MD5 (message digest) is primarily used to authenticate files.

This paper using MD5 for identity based encryption. There are two identities one is the order id and another is customer's id. (1001rajamohammed). this identification is converted to hash code (gcenkfhyjgenksfchk). And this hash code is used to encrypt the consumer's data. Then the consumers want to decrypt the data using same hash code.

It gives an error spotting capability. It is useful for storing a single-way hash of a password with key.

It comprises of 64 operations which is divided into 4 rounds of 16 operations. It handles a 128-bit which is splitted into four 32-bit which may be taken as A, B, C, D. There are 4 phases termed rounds in a message block.

The input message is divided into nuggets of 512-bit blocks.

The hash function has 2 conditions:

1. For producing a message matching a particular hash value must be impracticable for an intruder.

2. To produce 2 messages that creates the equal hash value must be impossible for an attacker.

The Message digests are one-way functions which are also known as hash functions.

In this algorithm, the message of any size as input is accepted and output is produced as a fixed-length message. (Sailee Wakhare et.al. [14]).

Steps

- First, we Initialize four Message digest buffers which are A, B, C, and D.
- A = 01 23 45 67.
  B = 89 ab cd ef.
  C = fe dc ba 98.
  D = 76 54 32 10.

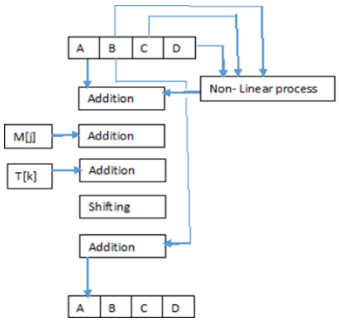

Fig. 5: MD5 Algorithm illustration

- B, C, and D are taken up for a non-linear process.
- A is then added.
- Then addition takes place between values of the sub block and the result.
- Constant values are added for a specific iteration.
- A shifting is tested with the string.
- String is summed up with B value and in turn is stored in A.
- For every round of sub block, the non-linear process is different.

The advantages of md5 algorithm are:

- It is Easier to compare.
- It Stores passwords.
- Low memory is enough to integrate.
- It checks the integrity and ultimately, we can monitor the file corruption.

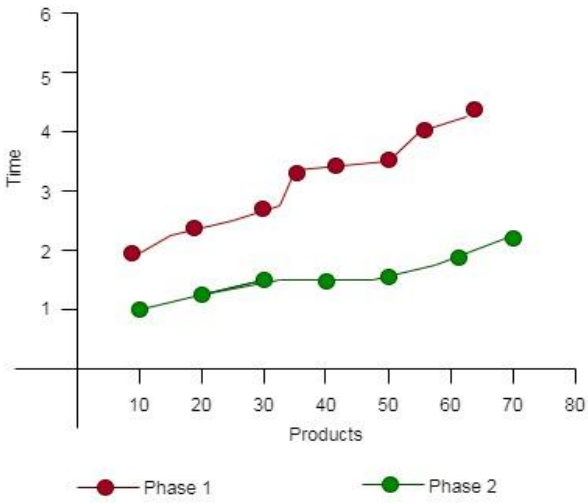

Fig. 6: Execution time graph for various products

RESULTS

Table 1: Phase 1 & Phase 2

Phase	Algorithm	Security	Time
Phase 1	AES Algorithm	Increase Production Using Security	1.0343 sec
Phase 2	AES, MD5 Algorithm	Increase Production using Security (AES with MD5)	0.321 sec

SAMPLE SCREENS

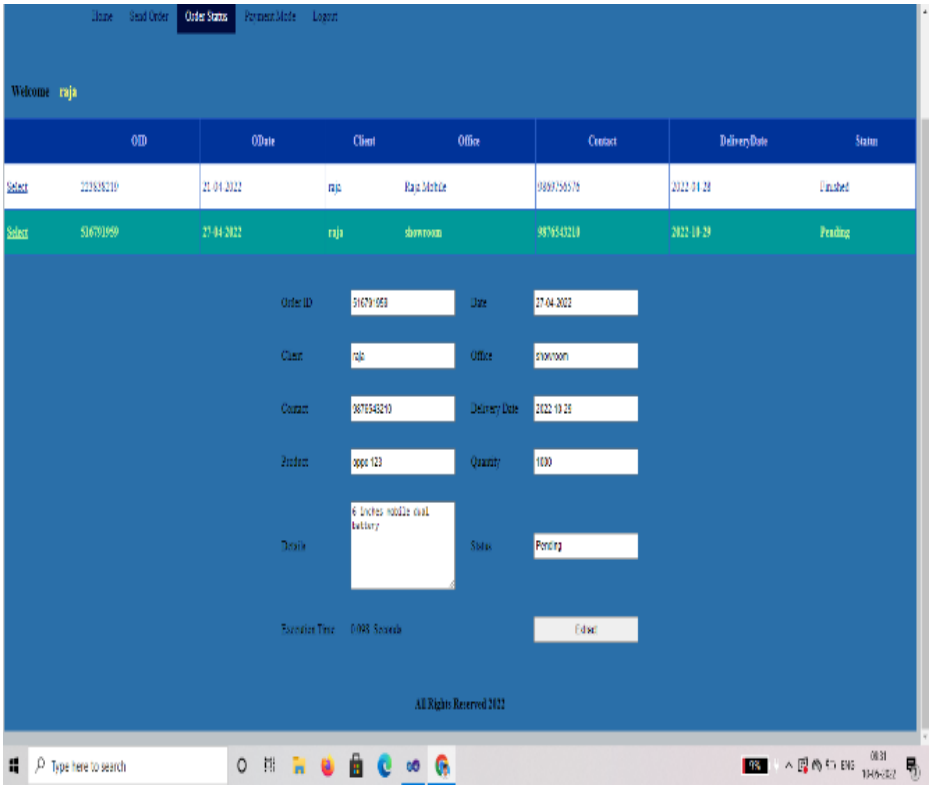

Fig. 7: Execution Time (0.098 seconds) showing encryption and decryption for data processing for a particular customer

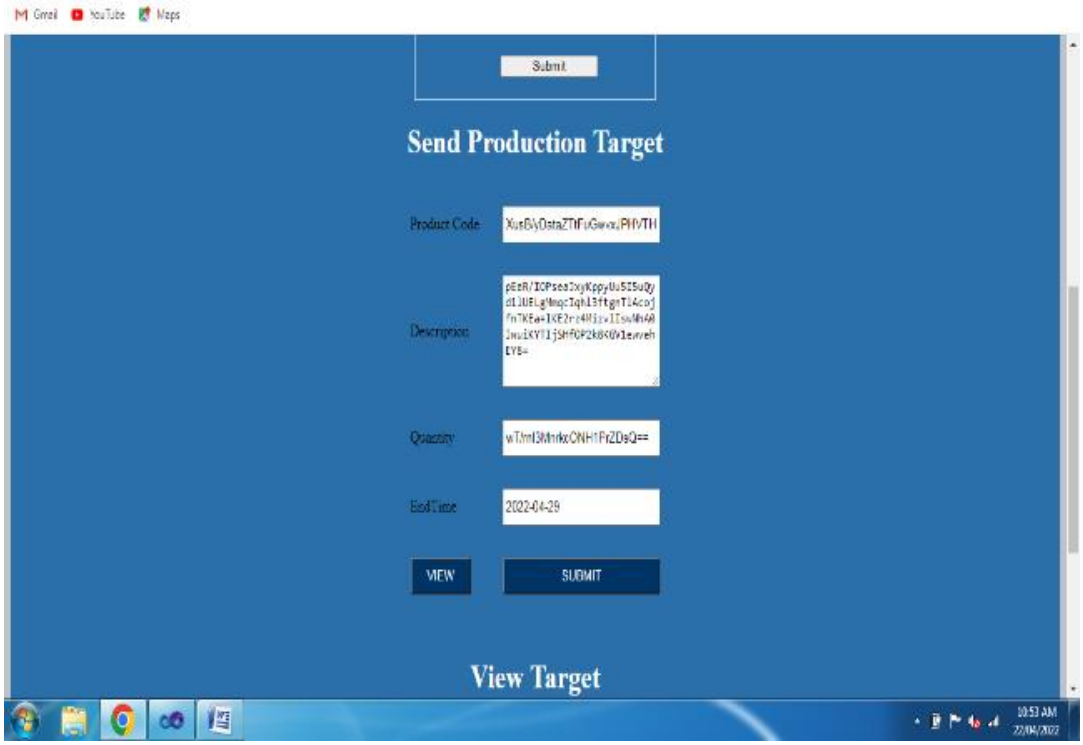

Fig. 8: View production details of encrypted data

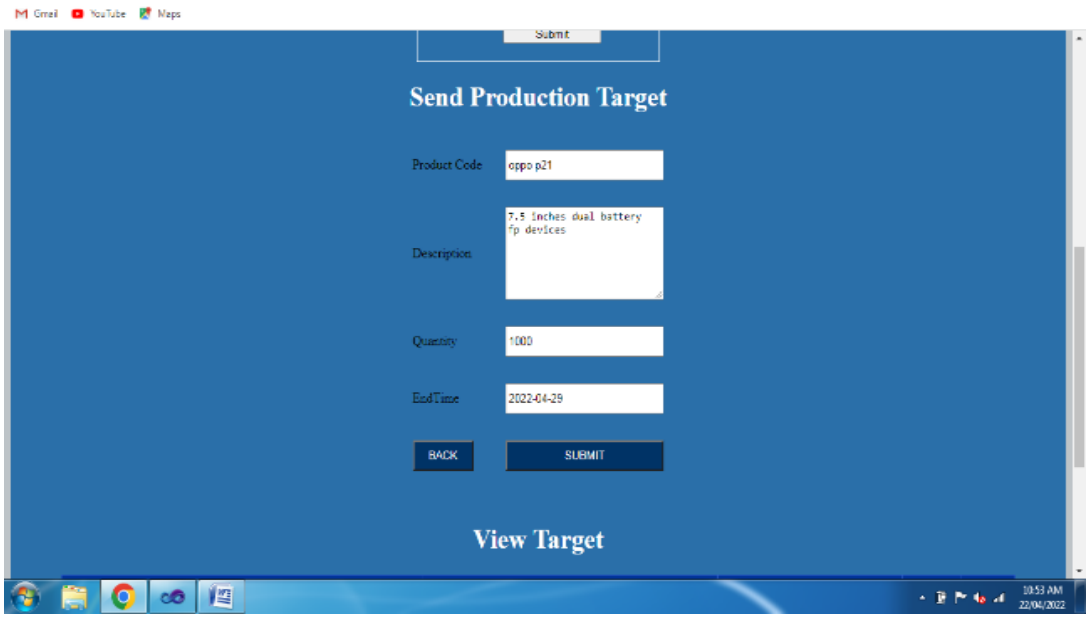

Fig. 9: View production details of decrypted data

CONCLUSION

In our paper, a structured analysis by PRISMA approach is carried out between the years 2012-2021 and concentrated on the IEEE Xplore database on the domain

of cyber security and data security in supply Chain Management. More systematic reviews can be done in other databases such as Scopus and Web of Science in future. The focus of this area was growing only after the year 2018. In addition, it is observed that, by the literature review, the applications of cryptography such as the encryption and decryption algorithms of data was not of much attention by researchers in SCM. To address this, we have incorporated AES 128- bit key algorithm and MD5 algorithm in SCM in this paper for securing the data. This will help the future researchers to conduct more studies.

REFERENCES

Jamaluddin, F., Saibani, N. Systematic Literature Review of Supply Chain Relationship Approaches amongst Business-to-Business Partners. Sustainability, vol. 13, 11935, pp. 1-25, 2021.

W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang and J. Han, "When Intrusion Detection Meets Blockchain Technology: A Review," in IEEE Access, vol. 6, pp. 10179-10188, 2018.

F. Fraile, T. Tagawa, R. Poler and A. Ortiz, "Trustworthy Industrial IoT Gateways for Interoperability Platforms and Ecosystems," in IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4506-4514, Dec. 2018.

U. Bodkhe et al., "Blockchain for Industry 4.0: A Comprehensive Review," in IEEE Access, vol. 8, pp. 79764-79800, 2020.

A. Shahid, A. Almogren, N. Javaid, F. A. Al-Zahrani, M. Zuair and M. Alam, "Blockchain-Based Agri-Food Supply Chain: A Complete Solution," in IEEE Access, vol. 8, pp. 69230-69243, 2020.

N. Gupta, A. Tiwari, S. T. S. Bukkapatnam and R. Karri, "Additive Manufacturing Cyber-Physical System: Supply Chain Cybersecurity and Risks," in IEEE Access, vol. 8, pp. 47322-47333, 2020.

G. Epiphaniou, P. Pillai, M. Bottarelli, H. Al-Khateeb, M. Hammoudesh and C. Maple, "Electronic Regulation of Data Sharing and Processing Using Smart Ledger Technologies for Supply-Chain Security," in IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1059-1073, Nov. 2020.

S. Cha, S. Baek and S. Kim, "Blockchain Based Sensitive Data Management by Using Key Escrow Encryption System From the Perspective of Supply Chain," in IEEE Access, vol. 8, pp. 154269-154280, 2020.

M. Asante, G. Epiphaniou, C. Maple, H. Al-Khateeb, M. Bottarelli and K. Z. Ghafoor, "Distributed Ledger Technologies in Supply Chain Security Management: A Comprehensive Survey," in IEEE Transactions on Engineering Management, pp.1-27, 2021.

V. Mullet, P. Sondi and E. Ramat, "A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0," in IEEE Access, vol. 9, pp. 23235-23263, 2021.

R. Pal et al., "Aggregate Cyber-Risk Management in the IoT Age: Cautionary Statistics for (Re)Insurers and Likes," in IEEE Internet of Things Journal, vol. 8, no. 9, pp. 7360-7371, 1 May1, 2021.

Ahmed Khan, D. Nour Moustafa, D. Pi, Y. Hussain and N. A. Khan, "DFF-SC4N: A Deep Federated Defence Framework for Protecting Supply Chain 4.0 Networks," in IEEE Transactions on Industrial Informatics, 2021.

L. Harikrishnan, Komal Arora, “Implementation of Advance Encryption Standard (AES) to Securely Store and Maintain Research Data”, International Journal of Engineering Technology, Management

and Applied Sciences, Volume 5, Issue 4, pp.127-130, 2017.

Sailee Wakhare, Priya Pise, Rutuja Khalate, Shivani Birajdar, Sonali Survase, “Secure Login System using MD5 and AES Attribute Based Encryption Algorithm”, International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume 9, Issue 8, pp.810-814, June 2020.

Ibrahim, S. (2022). Mathematical Modelling and Computational Analysis of Covid-19 Epidemic in Erbil Kurdistan Using Modified Lagrange Interpolating Polynomial. International Journal of Foundations of Computer Science, 1-17.