International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7422
***Article Received**: 07 May 2023 **Revised:** 27 June 2023 **Accepted:** 28 July 2023*

An Improved Integrity-Based Hybrid Multi-User Data Access Control for Cloud Heterogeneous Supply Chain Databases

Mani Deep Karumanchi[1], J. I. Sheeba[2], S. Pradeep Devaneyan[3], Lakshminarayana Kodavali[4]
[1]Department of Computer Science and Engineering
Bapatla Engineering College
Bapatla, A.P., India
manideep.karumanchi@becbapatla.ac.in
[2]Department of Computer Science and Engineering
Puducherry Technological University
Puducherry, India
sheeba@ptuniv.edu.in
[3]Department of Mechanical Engineering
Sri Venkateshwaraa College of Engineering and Technology
Puducherry, India
pr.signs@gmail.com
[4]Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation
Vaddeswaram, A.P., India
kodavali.lakshmi@kluniversity.in

Abstract— Cloud-based supply chain applications play a vital role in the multi-user data security framework for heterogeneous data types. The majority of the existing security models work effectively on small to medium-sized datasets with a homogenous data structure. In contrast, Supply Chain Management (SCM) systems in the real world utilize heterogeneous databases. The heterogeneous databases include a massive quantity of raw SCM data and a scanned image of a purchase quotation. In addition, as the size of the database grows, it becomes more challenging to provide data security on multi-user SCM databases. Multi-user datatypes are heterogeneous in structure, and it is complex to apply integrity and confidentiality models due to high computational time and resources. Traditional multi-user integrity algorithms are difficult to process heterogeneous datatypes due to computational time and variation in hash bit size. Conventional attribute-based encryption models such as "Key-policy attribute-based encryption" (KP-ABE), "Ciphertext-Policy Attribute-Based Encryption" (CP-ABE) etc., are used to provide strong data confidentiality on large textual data. Providing security for heterogeneous databases in a multi-user SCM system requires a significant computational runtime for these conventional models. An enhanced integrity-based multi-user access control security model is created for heterogeneous databases in the cloud infrastructure to address the problems with heterogeneous SCM databases. A non-linear integrity model is developed to provide strong integrity verification in the multi-user communication process. A multi-user based access control model is implemented by integrating the multi-user hash values in the encoding and decoding process. Practical results proved that the multi-user non-linear integrity-based multi-access control framework has better runtime and hash bit variation compared to the conventional models on large cloud-based SCM databases.

Keywords- Heterogeneous Supply Chain Data; Attribute-Based Encryption (ABE); Dictionary Encoding; Integrity Algorithm; Cloud Computing.

I. INTRODUCTION

Cloud computing involves one or more servers computing for other servers connected over the Internet [1]. The pay-per-use model used by cloud providers means that anyone who wants to use their IT services must pay only if they actually use them [2]. Processing power is one of the services offered, as is infrastructure for various web applications, including their development, testing, and hosting, as is the case with Amazon EC2 and Google AppEngine [3-4]. Despite its positive reputation, cloud computing has a number of serious privacy and security concerns that prevent its use in sensitive settings. All of these privacy and security issues are problems that an organisation moving to a cloud computing model must deal with [5]. It is due to the implementation of virtualization and multitenancy concepts, as well as the dynamic data initialization, heterogeneity, and distributed nature of the cloud. Additionally,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7422
***Article Received**: 07 May 2023 **Revised:** 27 June 2023 **Accepted:** 28 July 2023*

even a single service running in the cloud may contain components from different trusted or untrusted domains. In this regard, cloud users are unaware of the physical location of their data and services because data and services in the cloud are stored on servers that are geographically dispersed throughout the globe.

The problem of authentication and access control is made more difficult by the numerous vulnerabilities and threats that are introduced by these issues. Data confidentiality [6] is the degree to which the system is able to protect data from malicious insiders or outsiders, and it refers to the protection of any sensitive information against unauthorized or unintended access. Increased unauthorized access is related to an increase in the number of accessing devices, the transfer of data control to the cloud, and the threat to data confidentiality [7]. Data confidentiality is regarded as a legal as well as a privacy issue. For instance, the HIPAA (Health Insurance Portability and Accountability Act) law in the United States has established the rules for maintaining the confidentiality of supply chain transaction information. Before storing the data on distant cloud servers, the Data Owners (DO) can ensure the confidentiality of their sensitive data by encrypting the information. CloudCmp is proposed for Comparing Public Cloud Providers [8]. CloudCmp is a system that compares cloud providers' costs and performance in a methodical manner. Based on metrics that take into account how a customer's performance is impacted CloudCmp tracks the different aspects of a cloud, such as elastic computing, persistent storage, and networking services.

JD Edwards has left a significant impact on the business landscape with the introduction of JD Edwards OneWorld, an innovative application that integrated all business operations into a single system. This pioneering approach has transformed the way businesses operate by optimizing their processes, reducing costs, and enhancing efficiency. As technology continues to evolve, JD Edwards has remained at the forefront of innovation, recognizing the increasing practicality of automation in enterprise operations. To ensure the successful implementation of an ERP program in a business, Abdel-Basset et al. have categorized techniques into three key areas: organisational, technological, and human [9]. By establishing two applications to create ERP strategies, including JD Edwards Financials, which replaced their outdated financial management framework, JD Edwards has demonstrated its commitment to providing businesses with advanced functionality and flexibility to stay competitive in today's fast-paced market. JD Edwards ERP has become an indispensable tool for businesses of all sizes looking to remain competitive [10]. The company's unwavering dedication to customer satisfaction and innovative technology guarantees that it will continue to be a top preference for businesses seeking an ERP solution that can help them stay ahead of the competition. The impact of JD Edwards on the business landscape is undeniable, and its continuous efforts to innovate and improve its offerings demonstrate its commitment to helping businesses succeed. After conducting a comprehensive analysis of the organization's needs and objectives, Microsoft Dynamics Customer Relationship Management was identified as the most suitable solution to replace the outdated Sales Force program.

The implementation of JD Edward's application was entrusted to a reliable service provider, who demonstrated their expertise by delivering the project within an impressive six-month timeline. To ensure a seamless transition and successful change management, the Microsoft Dynamics CRM project was strategically divided into two parts, with 60% outsourced and 40% domestically introduced. The initial stage of the CRM project focused on developing and establishing the fundamental organizational concepts required to support the new CRM framework. The organization's exceptional project management skills were demonstrated by completing this stage within an impressive three-month timeline. The second stage was more complex and involved extending the CRM program to fully replace the Sales Force system. Despite the anticipated longer duration of this stage, it was deemed necessary to achieve the project's objectives. The implementation of Microsoft Dynamics CRM marked a significant milestone for the organization, providing a robust foundation for future growth and success. The organization's strategic approach to project management was evident in the decision to outsource part of the implementation to a service provider and domestically introduce the remaining part [11]. The new system was expected to streamline customer relationship management, enabling the organization to provide more efficient and effective services, which is vital for the organization's continued success. Overall, the implementation of Microsoft Dynamics CRM was a testament to the organization's commitment to innovation and excellence. The project's success was a result of the organization's exceptional project management skills, strategic approach, and collaboration with a reliable service provider. The new system was expected to provide a solid foundation for future growth and success, enabling the organization to continue providing exceptional services to its customers. The project has successfully progressed into its second stage and is expected to be completed within the next six months.

The ERP strategies have played a pivotal role in shaping and directing the variables that constitute the ERP aspect of the adoption model. To ensure a successful implementation of an ERP system, it is imperative to employ a combination of technical and organizational strategies [12]. Technical strategies focus on software implementation, while organizational strategies center around the people and processes involved in the adoption process. The implementation's success is dependent on various factors, including the quality of the software, the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7422
***Article Received**: 07 May 2023 **Revised:** 27 June 2023 **Accepted:** 28 July 2023*

proficiency of the implementation team, and the level of support from senior management. Furthermore, seamlessly integrating the system with existing business processes is of utmost importance to maximize the system's potential benefits [13]. Adopting an ERP system can bring about numerous advantages to a company, such as enhanced operational efficiency, better decision-making, and improved customer service. However, meticulous planning and attention to detail are essential to ensure a favorable outcome during the implementation process [14-15].

II. RELATED WORKS

CloudCmp strives to ensure compliance, fairness, and representativeness in its measures while working within the constraints of measurement cost. Through its application to various well-known cloud providers that account for a significant portion of cloud customers today, research has revealed that these providers offer varying services based on performance and price. This platform helps users choose the best provider for their specific needs according to the given specifications. Case studies of typical cloud applications have demonstrated the effectiveness of CloudCmp in aiding customers with provider selection. However, issues regarding data location and security are highlighted in cloud computing, as discussed in [16-17].

Deep et al., discusses the environmental issues related to data location and transmission, including legal restrictions and end-user demands for data storage within their nation [18]. The transfer of data from one country to another may result in these legal risks because different countries have different policies, regulations, and laws governing data creation, usage, and storage. The availability of data is yet another major problem; when data is unavailable, services or applications go down, which can result in a loss of customers and, consequently, money and loyalty [18]. This research paper discusses a further security concern, namely data security in mobility, which refers to the idea that when data mobility is high, security risks are also increased, particularly when data is transmitted between two countries that have different regulatory frameworks.

The different security issues covered by most authors are confidentiality and integrity. PDP [19], POR [20], Scalable PDP [21], Dynamis PDP, and HAIL are just a few of the approaches covered by the authors when it comes to data integrity. Author of this publication talks about cloud privacy and accountability [22]. It provides a very good overview of different methods for enforcing privacy, such as information-centric security, trusted cryptographic protocols, and computing. In order to achieve their desired results, they must quickly perform formal analyses to check for protocol failures and formulate protocol specifications based on the anticipated properties.

The emergence of cloud computing has significantly transformed the way data is stored and managed, providing numerous benefits for businesses and organizations. However, this technology also brings forth significant risks to data privacy and security, making it crucial to develop effective measures to mitigate these risks.

Belguith and their research team conducted a study to examine the impact of supply chain management (SCM) on procurement methods and related challenges [23]. The study revealed that information systems, information-sharing cooperation, and trust are critical issues that require attention. It is worth noting that supply chain management goes beyond a single business and necessitates coordination among all channel players. Furthermore, it plays a pivotal role in linking essential roles, procedures, and resources within and among channel members [24]. Although there is some research on how provider growth and supply incentives can encourage suppliers to adopt eco-friendly programs, more empirical evidence is required to determine their effectiveness in promoting sustainability in supply chains.

Belguith et al.'s study highlights the importance of addressing the challenges of information systems, information-sharing cooperation, and trust in supply chain management. Effective supply chain management is crucial for businesses to remain competitive in today's global economy. However, further research is needed to determine whether eco-friendly programs are a viable solution for enhancing sustainability in supply chains. The study's findings provide valuable insights for businesses seeking to improve their supply chain management practices and address the challenges they face. Addressing SCM challenges requires promoting transparency and accountability within supply chains and fostering collaborative efforts with vendors to ensure that their practices align with their product claims [25]. Another challenge of SCM is the systems' complexity, which can vary widely across different regions, languages, and cultural contexts. To overcome these challenges, stakeholders must engage in collaborative efforts and remain open to new ideas and approaches. By prioritizing transparency and accountability within supply chains and adapting to local conditions, we can continue to make progress toward a more sustainable future. This requires ongoing research and development of innovative strategies that are tailored to the unique needs and characteristics of different communities and regions.

The integration of external supply chain partners is a complex undertaking that presents several challenges, including navigating regulatory requirements, technical specifications, and a lack of specialized knowledge [26]. Overcoming these obstacles requires a significant financial investment to ensure a seamless integration process. However, the lack of motivation or cooperation from partners can hinder the efficient transfer of knowledge, information, and technology. Nonetheless, supplier integration is a vital component for the survival of the supply

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7422
***Article Received**: 07 May 2023 **Revised:** 27 June 2023 **Accepted:** 28 July 2023*

chain, as it enhances the quality of the final product. This requires adept management of the intricacies of the supply chain and ensuring an uninterrupted flow of supplies, providing prospective productive capacity to all supply chain partners. Given the critical role of supply chain management (SCM) in business operations, organizations must allocate the necessary resources and implement effective processes to ensure the successful integration of their supply chain partners. This can lead to streamlined operations, reduced costs, and improved customer satisfaction, which are fundamental objectives for any business. As such, it is essential to conduct thorough research and analysis to develop an effective strategy for supplier integration and SCM optimization.

The growth of manufacturing-related operations, such as sourcing and procurement, has brought about an increased importance of supply chain management. This involves the coordination of activities related to the production and delivery of goods and services from the point of origin to the point of consumption [27]. In today's global economy, supply chain management is a critical aspect of business operations, enabling companies to optimize inventory levels, reduce lead times, and improve delivery times while also cultivating strong relationships with suppliers and customers. However, managing a supply chain can be a daunting task. Companies must be equipped to manage potential risks, including supply chain disruptions resulting from natural disasters or political instability, while also balancing the costs of inventory, transportation, and logistics to ensure profitability [28-30].

In conclusion, the expansion of manufacturing-related operations has underscored the significance of supply chain management. By mitigating risks, reducing costs, and enhancing customer satisfaction, companies can establish a more efficient and effective supply chain, ultimately improving their competitiveness in the global market. Supply chain management experts play a pivotal role in guiding companies through these challenges and optimizing their supply chain operations to achieve success. It is crucial for businesses to understand the importance of supply chain management in today's global economy and to prioritize its effective implementation as a key aspect of their overall strategy [27].

As the size of the data increases, most of the traditional text-based encryption models have a problem with computational time and memory for the encryption and decryption process. Also, these models require only a unique static key for the data decryption process.

III. PROPOSED FRAMEWORK

In the proposed framework, an advanced supply chain data security model is developed in the cloud computing environment. In this framework, supply chain data are used as input from the MOBIS in order to provide security in the cloud server. In this proposed approach, the supply chain data are taken in multiple data formats, such as textual records and scanned images.

The recording of transaction details in supply chain records is essential for gaining a comprehensive view of the business process. These records contain critical information, including quantity, cost, lot size, buyer's ID, and order date. By analyzing this raw data, it is possible to gain a better understanding of the inner workings of the supply chain. The salesmen's end-of-day sales information is transmitted to MOBIS, who then forwards it to JDE through IIB. JDE leverages this information to create corresponding traditional trade (TT) sales orders, which are crucial for promoting the seamless flow of the supply chain. To ensure the accuracy of the purchasing order data, we undertake a series of steps to validate and verify it. We compare sales orders between MOBIS and JDE, utilizing the Customer PO as a common entity to ensure that both systems have identical information. The data is meticulously scrutinized for accuracy and compliance with required standards, with any discrepancies promptly identified and rectified to maintain the smooth operation of the supply chain. Subsequently, we verify the purchasing order data to ensure its validity and reliability. Maintaining precise and current supply chain records is a critical factor in the success of any business.

By adhering to our outlined steps, we can validate and verify the purchasing order data, ensuring that any discrepancies are identified and corrected promptly. Our unwavering commitment to providing our clients with unparalleled supply chain management expertise and support remains steadfast, reflecting our dedication to ensuring the smooth functioning of their supply chain operations.

Purchase order(PO) Verification JDE

- To maintain the precision and consistency of data for purchase orders (POs) and receipts, organizations utilize an automated system. This system begins by importing an XML file into the program, and then inputting the XML data values into the header sales and detail sales tables (f57011 and f57012, respectively).Upon importing the data, it undergoes validation against the master data to ensure its accuracy. The EDI tables, which include the EDI header (f47011) and EDI detail (F47012), are then updated with a new processed flag. This flag serves as an indicator of the data's status, with E representing Error, P indicating Processed, and N signifying Not Processed.
- The utilization of an automated system and data validation against the master data helps to minimize the risk of errors and delays, guaranteeing the timely delivery of the correct goods or services at the appropriate cost. To ensure the accuracy and integrity of data management, it is crucial to adopt a streamlined

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7422
***Article Received**: 07 May 2023 **Revised:** 27 June 2023 **Accepted:** 28 July 2023*

approach that filters out records that do not meet specific flag values. This approach guarantees that only relevant data is processed, reducing the risk of errors and enhancing the reliability of the information.

- Once the data is processed, updating the flag value of the F47011 and F47012 tables to "P" is a critical step that provides a clear indication of the completion of the processing. This step also enables the tracking of data processing progress, facilitating easy monitoring of the data's evolution.
- Moreover, updating the flag value to "P" simplifies the tracking of any modifications made to the data, which is particularly vital for auditing purposes. This approach creates a transparent record of any changes made to the data, ensuring accountability and facilitating easy monitoring of the data's evolution.

As cloud-based supply chain management systems continue to gain popularity, experts are increasingly focused on improving their security and reliability. To achieve this, the authors have integrated purchasing order (PO) data and the user's purchasing order copy as essential inputs to the cloud data security system. A hybrid heterogeneous data integrity algorithm has been proposed by the authors in this work to guarantee the integrity of every user in the multi-user system. This model uses each user attributes integrity value as a policy for the multi-user data encryption process. To further enhance the security of the system, authors have developed a hybrid heterogeneous integrity-based multi-user encoding framework consisting of four critical phases: data preprocessing, key generation, data encryption, and data decryption. Figure 1 shows the overall proposed framework.

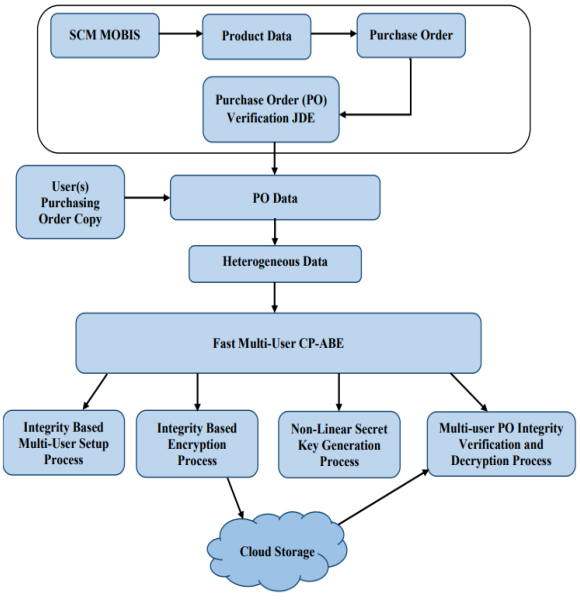

Figure 1. Proposed Framework

During the data preprocessing phase, authors convert the raw data into a structured format that is easily interpretable by the encryption algorithm. The key generation phase involves creating unique encryption keys for each user involved in the supply chain management process. Similarly, the decryption phase utiliz-es the same encryption keys to restore the data to its original state. This multi-user encryption process en-sures that the data remains safe and confidential, only accessible to authorized personnel.

The first phase of chain data involves a meticulous verification process that authorizes each user to ac-cess the data. This multi-user setup process is based on integrity, which guarantees that data is protected from unauthorized access and remains secure. The process ensures that only authorized users have access to the data, enhancing the security of the system.

The second phase of chain data employs advanced encryption techniques that provide a high level of se-curity during data storage and transfer. This integrity-based encryption process ensures that data is safe-guarded from tampering, alteration, or unauthorized access. The encryption process ensures that the data remains confidential and secure, even if it is intercepted during transfer.

The third phase of chain data generates complex secret keys using sophisticated algorithms. This non-linear secret key generation process enhances the security of data during storage and transfer by ensuring that the keys are not easily guessed or hacked. The process ensures that the data remains secure, even if the encryption key is compromised.

The final phase of chain data verifies the integrity of data during the purchase ordering process and de-crypts the data to make it accessible to authorized users. This multi-user purchase ordering integrity verifi-cation and decryption process ensures that data remains secure during the purchase process and is not tam-pered with or altered in any way as shown in figure 1.

A. Heterogeneous Data Integrity Algorithm

In this section, a hybrid heterogeneous integrity checking approach is developed in order to compute the unique hash value for the data encoding and decoding process. In this algorithm, a sequence of non-linear mathematical transformation steps is performed on the input data types for hash value computation. The proposed algorithm is shown below.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7422
Article Received: 07 May 2023 Revised: 27 June 2023 Accepted: 28 July 2023

Algorithm: Heterogeneous Data Integrity Algorithm

1: Initialization of Input.
for each product in the supply chain data **do**
S_id[] = getIds();
S_data[] = getData();
for each **id** in the **S_id[] do**
if (S_data=="Text") **then**
S_Bytes=S_id[i]+S_data;
else
S_Bytes[]=getBytes(S_Input); //Read data from Scanned PO Images
Done
Done
2: **Partition** the input data **M=S_data** into **k blocks** name it as **B[].**
3: **Pad message** if the length exceeds the block size with **0000001**
4: **for** each block in the B[] **do**
Partition the block into subblocks of size 32 bits to perform a sequence of mathematical transformations
Subblock partitions S_P[] = B[S/32];
for each sub-block in the **S_P[] do**
Perform nonlinearT(SP[i])
Done
Done
5: **Perform** non-linear sequence of transformation as **nonlinearT**
for each input byte in S_P[i] (sub-block partition byte array) **do**

$$mat\_y = |HS| . \frac{e^{-|\sum SK-\mu|/\rho}}{2\upsilon}; \upsilon > 0$$

μ = mean

η = det(mat_y);

$$gdf(\tau) = \frac{\lambda^{\alpha} x^{\alpha-1} e^{-\lambda\tau}}{\Gamma(\alpha)}, \quad \text{for } x > 0$$

$\psi(i)$ = subpart(i);

$m1 = \psi(i);$

$$m2 = \log\left(\frac{\lambda e^{-\lambda(\psi(i)-\tau)}}{(1+e^{-\lambda(\psi(i)-\tau)})^2} * gdf(\tau).sd\right)$$

$$m3 = \max\left(\frac{\lambda e^{-\lambda(\psi(i)-\tau)}}{(1+e^{-\lambda(\psi(i)-\tau)})^2} * gdf(\tau).var, mat\_y\right)$$

$Hash[i] = m1 \wedge m2 \wedge m3$

Done
6: **Final Hash (H)** = (Hash [0] || Hash [1] || Hash [2] ||……|| Hash [n**]);**

Description: In step 1, input data is converted into a byte array using the supply chain user ID as S_id and its corresponding record as S.data. This step is repeated for each multi-user data in the given transactions list. In step 2, input data M is partitioned into k blocks with each size 64 bits. In step 3, the padding operation is performed on the input data if the message_size exceeds the block size. In step 4, each block in the k blocks is partitioned into subblocks of each 32 bits. In step 5, a sequence of mathematical transformations is applied to the sub-block partition for hash computation. In step 6, all the subblock hash values are concatenated as the final hash value.

B. Fast multi-user CP-ABE model

In the proposed framework, a hybrid multi-user based supply chain framework is implemented on the different transaction data. In this approach, different key phases included: multi-user SCM key initialization, SCM data encryption, SCM-secret key generation, SCM-secret key decryption.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7422
***Article Received**: 07 May 2023 **Revised:** 27 June 2023 **Accepted:** 28 July 2023*

Multi-user setup process: In this step, different integrity sizes such as 512,1024,2048,4096 etc. are used to generate public key and master key for the secret key generation. Here, $G1, G2, Zp$ represents the cyclic group elements for key initialization process.

$Let \mathrm{G}_1, G_2, Z_p\ are$ randomized cyclic bilinear pairing numbers

$KS = U_r\{H(512), H(1024), H(2048), H(4096)\};$

In this phase, a hybrid master-key and public-key are evaluated using the cyclic group elements, bilinear pairing and mathematical distributions as given below.

$GD(r) = h(1-h)^p,$ p = 0,1,2, ...

$UD(r) = 1/(b\,1 - b2)$ for b1 $\leq m \leq b2$

Let Zr,G1,G2 are cyclic group elements and random elements.

CyclicGElement α = bi_pair(Zr,$\sigma_{GD(r)}$);

PubK.g = bi_pair(G1(), $\mu_{UD(m)}$);

PubK.gp = bi_pair(G2,r);

MasK.β = bi_pair(G2,r);

MasK.g_α = bi_pair(PubK.gp,$(\alpha)^{Zr}$;

PubK.h = bi_pair($(\beta)^{Zr}$,PubK.g);

PubK.g_$\hat{\alpha}$ = bi_pair(MasK.g_α,PubK.g,);

Multi-user-encryption: In this phase, a randomized cyclic group elements are used along with the cloud instance id and the cloud server name for the data encryption process. In this model, 4096 hash bit key is used to improve the overall security of the encoded data.

$$c1 = \mathrm{H}_{4096}(\alpha * \mathrm{c\_id});$$

$$c2 = \mathrm{H}_{4096}(\beta * \mathrm{c\_name});$$

Here α, β randomized cyclic group elements with multiplicative order. Here C1 and C2 are the encoded data using access tree policies and random cyclic group elements.

$Cipher\_Text(CT) = \{c1, c2,$

$cs = \{g\_alpha.(Zn)s, m.K\}, Atree,$

$c = \{Pbk.h.(Zn)\}, \quad T\}$

Non-linear private key generation: In this phase, a set of attributes and integrity values as policies and master_key are used to construct a complex private key for the decryption process. The multi-user secret key is generated by using the following metrics as.

$Let\ H\_Attlist$ is the 4096 value of all the supply chain purchasers list.

G1,G2 are the cyclic groups

A set of random generators from cyclic groups are r, g_r, g_p, r_j

$Cauchy$ distribution=CD$(d) = \dfrac{q}{\pi[(d-p)^2 + q^2]}$

Cyclic_Element g_r = Bipair(Zr);

Cyclic_Element Ahash = Bipair(G1,bytes($H\_Attlist[i]$).CD(m) .getBytes()).pow_Zn(rj));

SecrK.attr = $Attlist[i]$;

SecrK.Dj = {g_r.mul($H\_Attlist$)};

SecrK.Dj* = PK.gp.powZn(r_j);

$Secretkey$ = {g_r,SecrK.attr, $Attlist$, S ecrK.Dj,SecrK.Dj*, $H\_Attlist$}

Multi-user PO integrity verification and decryption: To decode the input data during the decryption phase, cypher text, secret key, Access tree, and policies are used.

IV. EXPERIMENTAL RESULTS

Experimental results are performed on different textual datasets using the java programming environment and third-party java libraries such as Java Agent Development Framework (JADE), Java Matrix (JAMA), Java Elliptic Curve Cryptography project (JECC), Amazon Web Services Java Development Kit (AWS JDK) etc. Amazon cloud storage is used to store the cipher text and secret key for data decryption process. In this experimental results, various performance metrics such as data size, sensitivity(mean change in bits), runtime are used to compare the performance of the proposed approach to the conventional approaches. Sensitivity represents the measuring the impact on the integrity bits by changing input data bits. Here, the runtime is computed for the integrity computational and data encryption and decryption process.

Mean change in bits: $MB = \frac{1}{N}\sum_{i=1}^{N} B_i$

Runtime (ms)= Final execution time(ms)- initial starting time(ms)

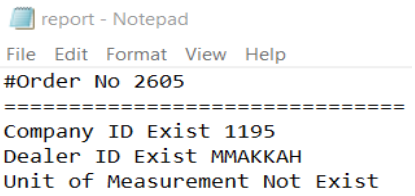

Figure 2. Sample Exception report for the inbound data validations

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7422
***Article Received**: 07 May 2023 **Revised:** 27 June 2023 **Accepted:** 28 July 2023*

TABLE I. SAMPLE F57011 DATA IN INBOUND AUTOMATION

FirmID	DealerID	CustomerID	AgentID	OrderID	OrderDate	ShippingDate	Total
1195	MMAKKAH	235133	436	119	20/12/2016	17/01/2017	32342
1195	MMAKKAH	235134	437	155	30/01/2017	30/01/2017	437
1195	MMAKKAH	235135	438	1085	18/07/2017	18/07/2017	454
1195	MMAKKAH	235136	439	1085	18/07/2017	18/07/2017	3233
1195	MMAKKAH	235137	440	2252	14/02/2017	14/05/2017	440
1195	MMAKKAH	235138	441	2464	18/03/2018	18/03/2018	64545
1195	MMAKKAH	235139	442	2464	18/03/2018	18/03/2018	5444
1195	MMAKKAH	235140	443	2464	18/03/2018	18/03/2018	7454
1195	MMAKKAH	235141	444	2481	21/03/2018	21/03/2018	444
1195	MMAKKAH	235142	445	2513	31/01/2017	31/03/2017	445
1195	MMAKKAH	235143	446	2605	23/04/2018	23/04/2018	446
1195	MMAKKAH	235144	447	2605	23/04/2018	23/04/2018	447
1195	MMAKKAH	235145	448	2605	23/04/2018	23/04/2018	448
1195	MMAKKAH	235146	449	2605	23/04/2018	23/04/2018	449
1195	MMAKKAH	235147	450	2605	23/04/2018	23/04/2018	450

TABLE II. SAMPLE F57012 DATA IN INBOUND AUTOMATION

CompanyID	Order Detail ID	ProductNo	Unit	Quantity ord	Quantity Ship	Price	Row no	Create Date	Document invoice	Refpo
1195	119	FPULK215	CR	-700	-700	3000	1	30/12/2016	55	852311
1195	155	FPULK109	CR	-216.67	-216.67	3001	2	30/01/2017	57	852225
1195	1085	FPMCV20	CR	-300	-300	3002	1	28/02/2018	1517	851481
1195	1085	FPMCV21	CR	-300	-300	3003	2	28/02/2018	1517	851483
1195	2252	FPULK214	CR	200	200	3004	1	14/02/2018	1673	851485
1195	2464	FPULK237	CR	-25	-25	3005	1	31/03/2018	1586	851486
1195	2464	FPULK238	CR	-25	-25	3006	2	31/03/2018	1586	851488
1195	2464	FPULK162	CR	-50	-50	3007	3	31/03/2018	1586	851489
1195	2481	FPULK239	CR	-100	-100	3008	1	31/03/2018	1587	851490
1195	2513	FPULK141	CR	100	100	3009	1	31/03/2017	1793	851491
1195	2605	FPMCV19	CR	-75	-75	3010	2	31/08/2018	1972	852225
1195	2605	FPULK267	CR	-22.33	-22.33	3011	3	31/08/2018	1972	852311
1195	2605	FPULK245	CR	-18	-18	3012	4	31/08/2018	1972	852311
1195	2605	FPMCV26	CR	-10	-10	3013	5	31/08/2018	1972	852225
1195	2605	FPMCV28	CR	-5	-5	3434	6	31/08/2018	1972	851481

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7422
***Article Received**: 07 May 2023 **Revised:** 27 June 2023 **Accepted:** 28 July 2023*

TABLE III. SAMPLE F47011 DATA IN INBOUND AUTOMATION

FirmID	DealerID	CustomerID	AgentID	OrderID	OrderDate	ShippingDate	Total	ProcessedFlg
1195	MMAKKAH	235134	437	155	30/01/2017	30/01/2017	437	N
1195	MMAKKAH	235137	440	2252	14/02/2017	14/05/2017	440	N

TABLE IV. SAMPLE F47012 DATA IN INBOUND AUTOMATION

Company ID	Order Detail ID	ProductNo	Unit	Quantity ord	Quantity Ship	Price	Row no	Create Date	Document invoice	Refpo	Processed Flg
1195	155	FPULK109	CR	-216.67	-216.67	3001	2	30/01/2017	57	852225	N
1195	2252	FPULK214	CR	200	200	3004	1	14/02/2018	1673	851485	N

TABLE V. SAMPLE F4201 DATA IN INBOUND AUTOMATION

FirmID	DealerID	CustomerID	AgentID	OrderID	OrderDate	ShippingDate	Total
1195	MMAKKAH	235134	437	155	30/01/2017	30/01/2017	437
1195	MMAKKAH	235137	440	2252	14/02/2017	14/05/2017	440

Table 1 – 5 shows the different tables stored in JDE database. Figure 2. Shows the Sample Exception report for the inbound data validations, Figure 3 presents the Purchase ordering data in the cloud server and Figure 4 shows the Purchase ordering flags error report in the cloud server.

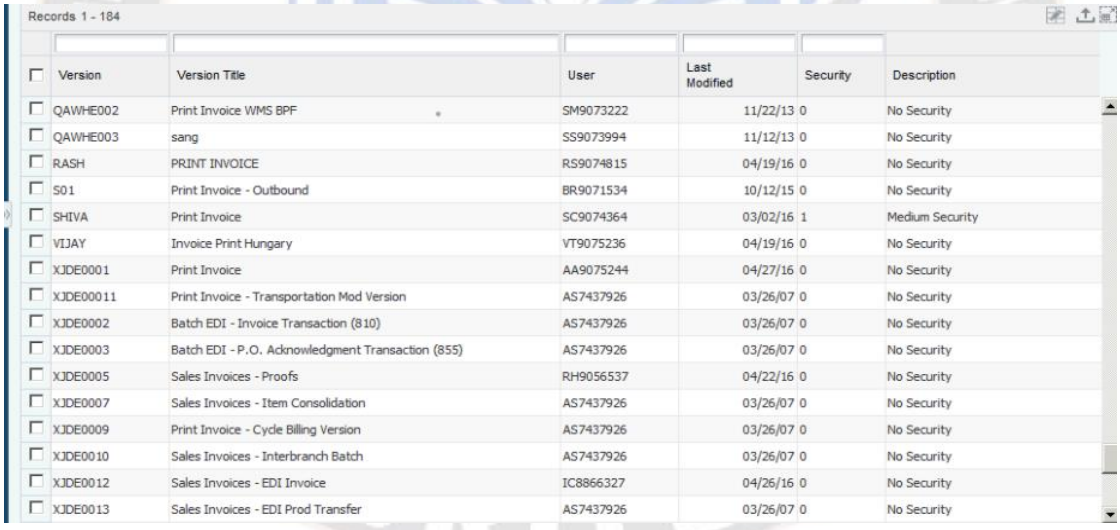

Figure 3. Purchase ordering data in the cloud server

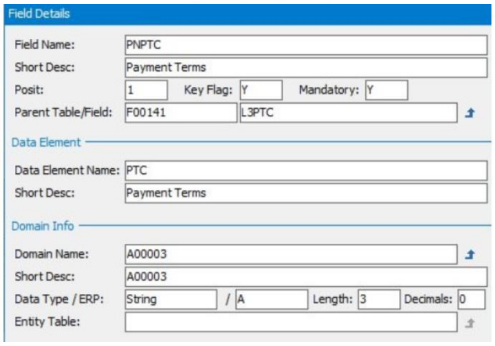

Figure 4. Purchase ordering flags error report in the cloud server

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7422
***Article Received**: 07 May 2023 **Revised:** 27 June 2023 **Accepted:** 28 July 2023*

Encryption and decryption computations are shown in Figure 5.

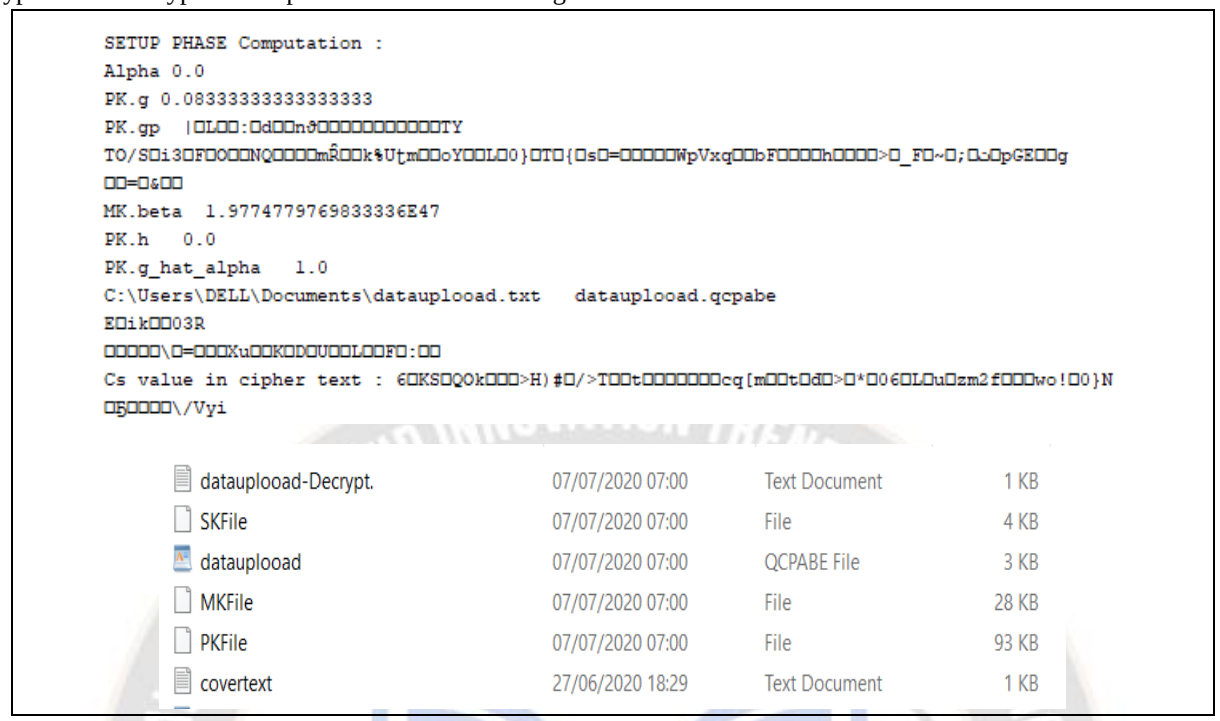

Figure 5. Encryption and Decryption

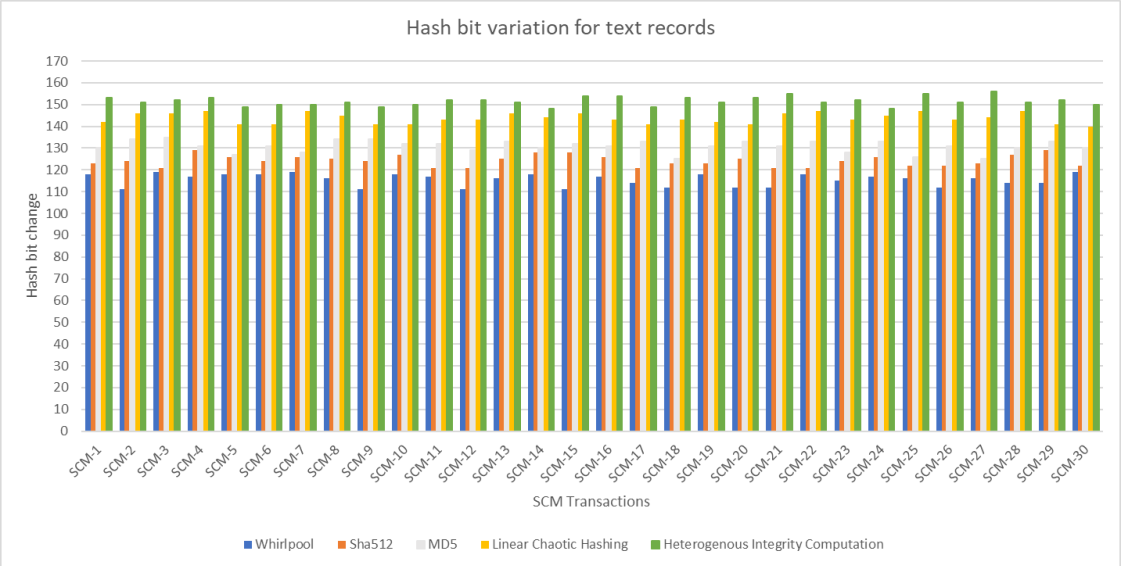

Figure 6. Hash bit change of proposed heterogeneous integrity verification model to existing hash based SCM approaches on variable size attributes with Textual data (Hash size=4096)

Figure 6, illustrates the hash bit variation of the heterogeneous integrity algorithm to the existing integrity approaches on different SCM textual transactions with variable size attributes. In this figure, it is noted that the proposed heterogeneous integrity model has better hash bit variation on different SCM transactions.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7422
***Article Received**: 07 May 2023 **Revised:** 27 June 2023 **Accepted:** 28 July 2023*

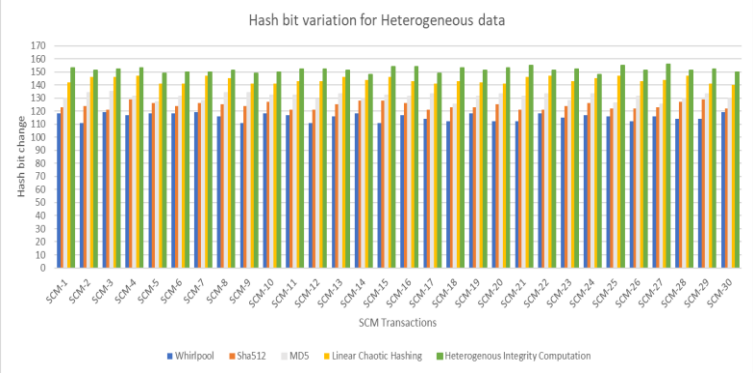

Figure 7. Hash bit variation of proposed heterogeneous integrity verification model to existing hash based SCM approaches on variable size attributes with heterogeneous datatype (Hash size =4096).

Figure 7, illustrates the hash bit variation of the heterogeneous integrity approach to the existing integrity approaches on different SCM transactions with variable size attributes. In this figure, it is noted that the proposed heterogeneous integrity model has better hash bit variation on different SCM heterogeneous data.

TABLE VI. PERFORMANCE ANALYSIS OF PROPOSED HETEROGENEOUS INTEGRITY MODEL AND CONVENTIONAL APPROACHES WITH VARYING ATTRIBUTES SIZE AND TEXTUAL DATA.

SCM Data	Whirlpool	SHA512	MD5	Linear Chaotic Hash	Heterogeneous Integrity Computation
SCM-1	3210	3173	2930	2949	**2475**
SCM-2	2825	3225	3190	2812	**2592**
SCM-3	3137	3158	2850	2884	**2351**
SCM-4	3104	2833	3111	3224	**2369**
SCM-5	3170	2880	2995	3178	**2582**
SCM-6	3046	3286	3142	3112	**2376**
SCM-7	3153	2989	3086	3074	**2293**
SCM-8	3009	3096	3234	2867	**2497**
SCM-9	3244	2890	3023	2891	**2548**
SCM-10	3231	3090	3097	3047	**2508**
SCM-11	2957	3021	3230	3235	**2342**
SCM-12	2883	3006	2997	3228	**2355**
SCM-13	2964	3117	3193	3005	**2495**
SCM-14	3215	2992	3092	2914	**2532**
SCM-15	2812	2952	3272	3142	**2492**
SCM-16	3134	3043	3078	2921	**2640**
SCM-17	3182	3269	2853	3070	**2645**
SCM-18	3004	2901	2928	2998	**2566**
SCM-19	3061	2999	2810	3140	**2411**
SCM-20	2910	2838	3260	2873	**2631**
SCM-21	2868	3042	3180	3157	**2589**
SCM-22	3204	3133	2895	2821	**2428**
SCM-23	3088	3229	2982	3151	**2670**
SCM-24	3161	2815	3083	3012	**2620**
SCM-25	2997	2941	3112	3023	**2587**
SCM-26	3119	2788	3168	2918	**2601**
SCM-27	3146	2857	3127	2980	**2535**
SCM-28	2968	2861	3110	3247	**2563**
SCM-29	3075	3234	3250	3018	**2330**
SCM-30	3150	2863	3271	2978	**2680**

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7422
***Article Received**: 07 May 2023 **Revised:** 27 June 2023 **Accepted:** 28 July 2023*

Table 6, represents the runtime analysis of proposed heterogeneous integrity model to the conventional models on SCM textual transactions data. In the setup, different attributes and transactions are used to compute the runtime of each transaction.

TABLE VII. PERFORMANCE ANALYSIS OF PROPOSED HETEROGENEOUS INTEGRITY MODEL AND CONVENTIONAL APPROACHES WITH VARYING ATTRIBUTES SIZE AND HETEROGENEOUS DATA.

SCM Data	Whirlpool	SHA512	MD5	Linear Chaotic Hash	Heterogeneous Integrity Computation
SCM-1	3195	2785	2857	3060	**2478**
SCM-2	3040	3091	3140	2978	**2654**
SCM-3	2837	3265	3095	2819	**2427**
SCM-4	3143	2982	3197	2807	**2653**
SCM-5	3270	3258	3117	2963	**2384**
SCM-6	3202	3042	2914	3135	**2563**
SCM-7	2827	2929	2854	2970	**2384**
SCM-8	3156	2944	3142	3121	**2515**
SCM-9	3107	3238	3206	3082	**2369**
SCM-10	3225	2960	3266	3071	**2561**
SCM-11	3223	3278	3133	2944	**2646**
SCM-12	2865	3131	2935	3164	**2323**
SCM-13	2955	2884	3133	2834	**2330**
SCM-14	3249	3079	2806	3030	**2522**
SCM-15	3238	2895	3036	3117	**2602**
SCM-16	3165	2889	3214	3169	**2456**
SCM-17	2982	2987	2963	3077	**2349**
SCM-18	2860	2839	2906	2931	**2667**
SCM-19	3256	2931	2836	3266	**2418**
SCM-20	2887	2948	3001	2831	**2533**
SCM-21	3283	3142	2973	3096	**2524**
SCM-22	2930	3017	3093	3237	**2676**
SCM-23	3051	2871	3059	2929	**2560**
SCM-24	2998	2921	3148	2808	**2308**
SCM-25	2784	2940	2925	2922	**2347**
SCM-26	3140	3226	3079	3100	**2685**
SCM-27	3229	3143	3018	3229	**2307**
SCM-28	2993	2790	2984	3028	**2483**
SCM-29	3000	3008	3055	3257	**2545**
SCM-30	**2908**	**3086**	**3078**	**3169**	**2676**

Table 7, represents the runtime analysis of the proposed heterogeneous integrity model to the conventional models on SCM heterogeneous data. In the setup, different attributes and transactions are used to compute the runtime of each transaction and heterogeneous data type.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7422
***Article Received**: 07 May 2023 **Revised:** 27 June 2023 **Accepted:** 28 July 2023*

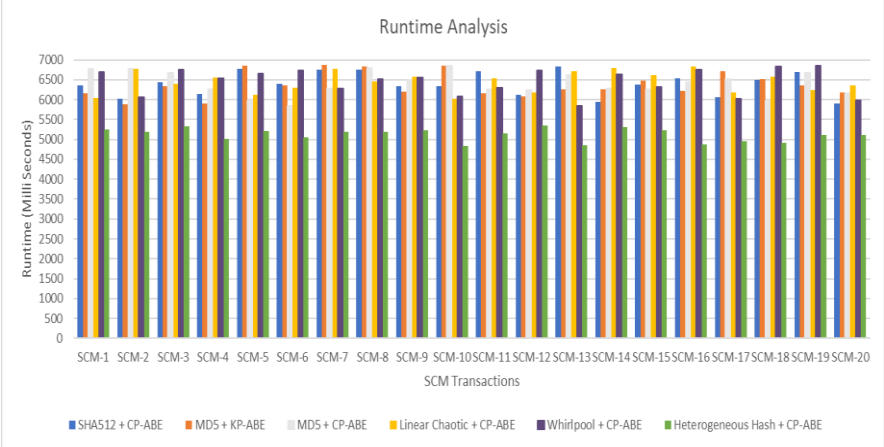

Figure 8. Comparison of proposed heterogeneous integrity based multi-user encoding model to traditional hybrid encoding models in terms of runtime analysis on heterogeneous data.

Figure 8, represents the runtime analysis of proposed non-linear integrity based encoding approach to the conventional approaches on SCM heterogeneous data. As shown in the figure, it is observed that the non-linear integrity based encoding and decoding approach has less runtime than the existing heterogeneous security models.

V. CONCLUSION

In this paper, a hybrid non-linear integrity based encoding and decoding framework is implemented on the homogeneous and heterogeneous SCM data types. Most of the conventional supply chain integrity approaches are difficult to process and provide strong security on the heterogeneous data types in the cloud computing environment. Also, traditional linear hashing approaches are vulnerable to man-in the middle attacks. In order to solve these problems, a nonlinear integrity based encoding and decoding framework is developed on the large SCM datatypes in the cloud server. In this work, a hybrid variable size non-linear integrity algorithm and hybrid attribute-based encoding and decoding approach are developed in order to improve the cloud data security on the heterogeneous data types. In future, this work can be extended to integrate non-linear hashing approach and proposed attribute based approach in the block chain technology.

REFERENCES

[1] Ali, S. I., Ali, A., AlKilabi, M., & Christie, M. (2021). Optimal supply chain design with product family: A cloud-based framework with real-time data consideration. Computers & Operations Research, 126, 105112, doi: 10.1016/j.cor.2020.105112.

[2] Karumanchi, M. D., Sheeba, J. I., & Devaneyan, S. P. (2019, December). Cloud based supply chain management system using blockchain. In 2019 4th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT) (pp. 390-395). IEEE, doi: 10.1109/ICEECCOT46775.2019.9114692

[3] Bergier, I., Papa, M., Silva, R., & Santos, P. M. (2021). Cloud/edge computing for compliance in the Brazilian livestock supply chain. Science of The Total Environment, 761, 143276, doi: 10.1016/j.scitotenv.2020.143276.

[4] Bose, R., Mondal, H., Sarkar, I., & Roy, S. (2022). Design of smart inventory management system for construction sector based on IoT and cloud computing. e-Prime-Advances in Electrical Engineering, Electronics and Energy, 2, 100051, doi: 10.1016/j.prime.2022.100051.

[5] Kamble, V. S. ., Khampariya, P. ., & Kalage, A. A. . (2023). A Survey on the Development of Real-Time Overcurrent Relay Coordination Using an Optimization Algorithm. International Journal of Intelligent Systems and Applications in Engineering, 11(3s), 104–114. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2537

[6] Karumanchi, M. D., Sheeba, J. I., & Devaneyan, S. P. (2022). Integrated Internet of Things with cloud developed for data integrity problems on supply chain management. Measurement: Sensors, 24, 100445, doi: 10.1016/j.measen.2022.100445

[7] Chen, L. M., & Chang, W. L. (2021). Supply-and cyber-related disruptions in cloud supply chain firms: Determining the best recovery speeds. Transportation Research Part E: Logistics and Transportation Review, 151, 102347, doi: 10.1016/j.tre.2021.102347.

[8] Chinnasamy, P., Padmavathi, S., Swathy, R., & Rakesh, S. (2021). Efficient data security using hybrid cryptography on cloud computing. In Inventive Communication and Computational Technologies: Proceedings of ICICCT 2020 (pp. 537-547). Springer Singapore, doi: 10.1007/978-981-15-7345-3_46

[9] Javed, B., Bloodsworth, P., Rasool, R. U., Munir, K., & Rana, O. (2016). Cloud market maker: An automated dynamic pricing marketplace for cloud users. Future Generation Computer Systems, 54, 52-67, doi: 10.1016/j.future.2015.06.004.

[10] Abdel-Basset, M., Gunasekaran, M., Mohamed, M., & Chilamkurti, N. (2019). A framework for risk assessment, management and evaluation: Economic tool for quantifying risks in supply chain. Future Generation Computer Systems, 90(1), 489-502, doi: 10.1016/j.future.2018.08.035.

[11] Longo, F., & Mirabelli, G. (2008). An advanced supply chain management tool based on modeling and simulation. Computers & Industrial Engineering, 54(3), 570-588, doi: 10.1016/j.cie.2007.09.008.

[12] Peiris, K. D. A., Jung, J., & Gallupe, R. B. (2015). Building and evaluating ESET: A tool for assessing the support given by an enterprise system to supply chain management. Decision Support Systems, 77, 41-54, doi: 10.1016/j.dss.2015.05.004.

[13] Yeh, T. M., Yang, C. C., & Lin, W. T. (2007). Service quality and ERP implementation: A conceptual and empirical study of semiconductor-related industries in Taiwan. Computers in Industry, 58(8-9), 844-854, doi: 10.1016/j.compind.2007.03.002.

[14] Hassan, R. S., Nawaz, A., Lashari, M. N., & Zafar, F. (2015). Effect of customer relationship management on customer satisfaction. Procedia economics and finance, 23, 563-567, doi: 10.1016/S2212-5671(15)00513-4.

[15] Silva Filho, O. S., & Neagu, G. (2000). Special Session on Models and Tools for Supply Chain Management. IFAC Proceedings Volumes, 33(17), 909-910, doi: 10.1016/S1474-6670(17)39524-1.

[16] Hartono, E., Holsapple, C. W., & Jin, H. (2011). The role of technological know-how in c-commerce success. Decision support systems, 51(1), 77-87, doi: 10.1016/j.dss.2010.11.030.

[17] AlAhmad, A. S., Kahtan, H., Alzoubi, Y. I., Ali, O., & Jaradat, A. (2021). Mobile cloud computing models security issues: A systematic review. Journal of Network and Computer Applications, 190, 103152, doi: 10.1016/j.jnca.2021.103152.

[18] Karumanchi, M. D., Sheeba, J. I., & Devaneyan, S. P. (2022). Nonlinear integrity algorithm for blockchain based supply chain databases. In Pervasive Computing and Social Networking: Proceedings of ICPCSN 2022 (pp. 169-181). Singapore: Springer Nature Singapore, doi: 10.1007/978-981-19-2840-6_13.

[19] Deep, G., Sidhu, J., & Mohana, R. (2022). Insider threat prevention in distributed database as a service cloud environment. Computers & Industrial Engineering, 169, 108278, doi: 10.1016/j.cie.2022.108278.

[20] Parast, F. K., Sindhav, C., Nikam, S., Yekta, H. I., Kent, K. B., & Hakak, S. (2022). Cloud computing security: A survey of service-based models. Computers & Security, 114, 102580, doi: 10.1016/j.cose.2021.102580.

[21] Li, R., Wang, X. A., Yang, H., Niu, K., Tang, D., & Yang, X. (2022). Efficient certificateless public integrity auditing of cloud data with designated verifier for batch audit. Journal of King Saud University-Computer and Information Sciences, 34(10), 8079-8089, doi: 10.1016/j.jksuci.2022.07.020.

[22] Nain, G., Pattanaik, K. K., & Sharma, G. K. (2022). Towards edge computing in intelligent manufacturing: Past, present and future. Journal of Manufacturing Systems, 62, 588-611, doi: 10.1016/j.jmsy.2022.01.010.

[23] Chinnasamy, P., & Deepalakshmi, P. (2022). HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud. Journal of Ambient Intelligence and Humanized Computing, 1-19, doi: 10.1007/s12652-021-02942-2

[24] Belguith, S., Kaaniche, N., Laurent, M., Jemai, A., & Attia, R. (2018). Phoabe: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted iot. Computer Networks, 133, 141-156, doi: 10.1016/j.comnet.2018.01.036.

[25] Mandal, M. (2020). Privacy-preserving fully anonymous ciphertext policy attribute-based broadcast encryption with constant-size secret keys and fast decryption. Journal of Information Security and Applications, 55, 102666, doi: 10.1016/j.jisa.2020.102666.

[26] Pareek, G., & Purushothama, B. R. (2020). Proxy re-encryption for fine-grained access control: Its applicability, security under stronger notions and performance. Journal of Information Security and Applications, 54, 102543, doi: 10.1016/j.jisa.2020.102543.

[27] La Manna, M., Perazzo, P., & Dini, G. (2021). SEA-BREW: A scalable attribute-based encryption revocable scheme for low-bitrate IoT wireless networks. Journal of Information Security and Applications, 58, 102692, doi: 10.1016/j.jisa.2020.102692.

[28] Sun, X., Wang, H., Fu, X., Qin, H., Jiang, M., Xue, L., & Wei, X. (2021). Substring-searchable attribute-based encryption and its application for IoT devices. Digital Communications and Networks, 7(2), 277-283, doi: 10.1016/j.dcan.2020.07.008.

[29] Abdul Rahman, Artificial Intelligence in Drug Discovery and Personalized Medicine , Machine Learning Applications Conference Proceedings, Vol 1 2021.

[30] Sun, P. (2020). Security and privacy protection in cloud computing: Discussions and challenges. Journal of Network and Computer Applications, 160, 102642, doi: 10.1016/j.jnca.2020.102642.

[31] Karumanchi, M. D., Sheeba, J. I., & Devaneyan, S. P. (2022). Blockchain enabled supply chain using machine learning for secure cargo tracking. International Journal of Intelligent Systems and Applications in Engineering, 10(4), 434-442.

[32] Karumanchi, M. D., Sheeba, J. I., & Devaneyan, S. P. (2023). An efficient integrity based multi-user blockchain framework for heterogeneous supply chain management applications. International Journal of Computers and Applications, 45(4), 337-351.doi: 10.1080/1206212X.2023.2199966.