IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 11, Issue 4, 2023

Innovative Cloud Computing Strategies for Automotive Supply Chain Data Security and Business Intelligence

Venkata Surya Bhavana Harish Gollavilli,

Under Armour, Maryland, USA

venkatasuryagollapalli@gmail.com

Kalyan Gattupalli,

Yash Tek inc,

Ontario, Canada

kalyaang2010@gmail.com

Harikumar Nagarajan,

Global Data Mart Inc (GDM),

New Jersey, USA

Haree.mailboxone@gmail.com

Poovendran Alagarsundaram,

Humetis Technologies Inc,

Kingston, NJ, USA

poovasg@gmail.com

Surendar Rama Sitaraman,

Samsung Austin Semiconductor LLC, Folsom, California, USA

sramasitaraman@gmail.com

ABSTRACT

The purpose of this project is to determine how the security, resilience, and efficiency of the automotive supply chain may be greatly improved by integrating cloud computing, IoT, blockchain, and advanced cryptographic techniques. In order to enhance decision-making and enable predictive maintenance, ideal inventory control, and faster logistics procedures, the architecture makes use of AI-powered analytics and real-time monitoring via IoT devices. Blockchain technology lessens the possibility of manipulation and fraud by guaranteeing the

transparency and integrity of supply chain transactions. By guaranteeing that only authorised personnel can access sensitive information, the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) paradigm reduces the danger of unauthorised access. Furthermore, excellent data security is provided by the architecture's non-linear hashing techniques and dynamic key creation, safeguarding vital supply chain data. Performance assessments show that the suggested non-linear hash model is more sensitive and efficient than traditional algorithms, which makes it especially suitable for the intricate and dynamic automotive supply chain environment. The findings demonstrate that the suggested design improves the overall operational efficiency and adaptability of the supply chain in addition to satisfying the industry's needs for scalable and secure data management solutions. The study does, however, also draw attention to the difficulties in integrating these cutting-edge technology, highlighting the necessity of continual managerial involvement and overcoming change-resistant behaviour for successful implementation.
Keywords: Cloud Computing, Blockchain, Automotive Supply Chain, Data Security, AI-Powered Analytics, Real-Time Monitoring.

1. INTRODUCTION

Integrating cloud computing has become essential for improving supply chain efficiency and guaranteeing data security in the quickly changing automotive sector. Numerous parties, including manufacturers, suppliers, dealers, and logistics companies, are involved in the automobile supply chain and handle enormous volumes of sensitive data. The requirement for real-time business analytics and strong data security has increased as the sector embraces digital transformation. Cloud computing can meet these objectives, which provides scalable, adaptable, and reasonably priced solutions that facilitate safe storage and easy data sharing throughout the supply chain. But given the dynamic nature of automotive data and the inherent complexity of cloud infrastructures, novel approaches are needed to reduce risks like data breaches, illegal access, and problems with data integrity. In order to improve supply chain operations, this study leverages business intelligence to use data security and examines innovative cloud computing solutions specifically designed for the automobile industry. The suggested tactics are designed to guarantee the availability, confidentiality, and integrity of data related to the automotive supply chain by utilising cutting-edge encryption techniques and integrating cloud-based IoT solutions. This will help to build a more robust and adaptable supply chain ecosystem.

The supply chain in the automotive sector has traditionally managed production, inventory, and distribution activities using conventional, centralised methods. Although useful in the past, these systems have found it difficult to keep up with the scale and complexity of the contemporary automotive supply chains. The emergence of cloud computing throughout the early 2000s brought about a notable change by providing a decentralised method that facilitates instantaneous data exchange and cooperation between supply chain members. Although cloud computing was once used for simple tasks like data storage, its use has grown to include complex supply chain management systems. But there are new difficulties as well because of the growing reliance on

cloud services, especially when it comes to protecting critical supply chain data and guaranteeing data security.

Cloud computing has advanced significantly in the automobile industry due to the demand for intelligent, scalable, and secure supply chain solutions. Blockchain, homomorphic encryption, and artificial intelligence (AI) are examples of cutting-edge technologies that are now integrated into modern cloud systems to improve data security and business insight. Homomorphic encryption addresses major issues about data security by enabling data to be handled without losing its confidentiality, while blockchain assures tamper-proof records of transactions. Furthermore, cloud systems with AI-driven analytics provide real-time decision-making and predictive insights, which greatly increase supply chain efficiency. By integrating Internet of Things (IoT) devices, data collecting and monitoring capabilities are further enhanced and a full view of the entire supply chain is provided. Together, these developments provide the automobile industry the ability to create supply chains that are more responsive, transparent, and safe.

- Improve Data Security: Create cloud-based plans to guard against hacks and illegal access to data related to the automotive supply chain.
- Boost Data Integrity: To guarantee the precision and consistency of supply chain data, use blockchain technology and cutting-edge encryption techniques.
- Leverage Business Intelligence: To improve operational efficiency and decision-making in the automotive supply chain, make use of AI and cloud-based analytics.
- Allow for Real-Time Cooperation: Enable secure cloud platforms to facilitate smooth data sharing and collaboration among supply chain stakeholders.
- Strengthen Supply Chain Resilience: By combining cloud computing and IoT for real-time monitoring and reaction, you can create a supply chain that is more adaptive and resilient.

In the context of cloud services and corporate analytics, the research paper discusses the urgent need for digital transformation in supply chain management, Tozin and Amaro (2022). Digitisation helps the automobile industry tremendously by improving the responsiveness and efficiency of the supply chain, two things that are essential for keeping a competitive advantage. But there are a lot of obstacles to overcome when integrating Business Intelligence (BI) tools with supply chain management. The lack of enthusiasm and involvement from managers, who are essential to the effective implementation and optimisation of new technologies, is a major problem. The full potential of BI systems in sustaining competitive advantage and encouraging innovation in the supply chain is unrealised in the absence of proactive managerial engagement. In order to enable a more efficient and data-driven supply chain ecosystem, this project intends to investigate the obstacles to effective managerial engagement and suggest solutions.

Pattnaik et al. (2022), despite the potential of cloud computing, business intelligence, and sophisticated technologies such as blockchain and AI to improve data security and operational efficiency in automotive supply chains, significant gaps still exist. Specifically, there has been

ISSN 2347–3657
Volume 11, Issue 4, 2023

insufficient research on how managerial engagement influences the uptake and optimisation of these technologies. Although the benefits of cloud-based solutions and business intelligence tools are generally understood, the role of managerial engagement in overcoming opposition to change and ensuring effective implementation is understudied. Furthermore, much current research overlooks the actual application of improved encryption and IoT for real-time data sharing. This study aims to fill these gaps by exploring the impact of managerial participation in technological adoption and offering ways to build a more resilient and adaptable supply chain ecosystem.

2. LITERATURE SURVEY

The integration of business intelligence (BI) tools to improve supply chain management (SCM) operations is examined by Tozin and Amaro (2022). It demonstrates how supply chain operations may be optimised by BI technology through increased efficiency, real-time decision-making, and improved data visibility. In the context of the supply chain, the study highlights the use of business intelligence (BI) in predictive analytics, trend analysis, and risk management. It also shows how these technologies can result in better decisions, lower costs, and more efficient operations. The study highlights its conclusions with case studies and real-world applications.

Rajya Lakshmi Gudivaka (2021) proposed a dynamic four-phase cloud data security system using LSB steganography and cryptography. Data gets encrypted and hidden in the pixels of an image, and AES keys get secured through RSA and embedded in a cover object. This framework enhances cloud security by giving secrecy, integrity, and redundancy while suggesting future improvements by using machine learning and finer steganalysis methods.

According to Pattnaik et al. (2022), artificial intelligence (AI) is transforming supply chain management in dynamic corporate settings. It presents a novel approach that uses AI technology to improve supply networks' responsiveness, flexibility, and efficiency. Predictive analytics powered by AI for demand forecasting, work automation, and sophisticated decision-making are some of the standout features. In addition, the paper examines how AI may enhance supply chain resilience, agility, and cooperation while showcasing cutting-edge AI solutions that promote operational excellence and competitive advantage.

Narla et al. (2019) examine progress in digital health technologies, emphasising the integration of machine learning with cloud-based systems for risk factor assessment. They emphasise current deficiencies in real-time data processing and pattern recognition. Their literature review highlights the efficacy of LightGBM, multinomial logistic regression, and SOMs in achieving precise forecasts and personalised healthcare, thereby reconciling data complexity with decision-making.

Sharadha Kodadi (2022) explores the integration of cloud computing with advanced tools like wavelet analysis, big data analytics, and machine learning to enhance real-time seismic data processing. The proposed system improves earthquake prediction, data management, and coordination in dealing with the challenges that characterize the traditional systems and significantly boost disaster response and recovery efforts.

Golightly et al. (2022) analysis looks at how businesses use cloud computing as a major breakthrough to improve their operations. It draws attention to the tactical advantages of cloud adoption, including improved flexibility, cost-effectiveness, and scalability. The study focusses on the ways that cloud computing helps businesses to accelerate digital transformation, enhance collaboration, and modernise their IT infrastructure. The influence of cloud technologies on organisational agility, competitive advantage, and innovation capability, as well as implementation and management problems, are among the key results. The article offers advice on successful cloud adoption strategies and success factors.

Akhil Raj Gaius Yallamelli (2021) used Content Analysis, PLS-SEM, and CART to examine the influence of cloud computing on SMEs' management accounting. It has brought about real-time data access, better decision-making, and regulatory compliance. While it offers sophisticated analytics, it also faces issues related to data security, privacy, and training of employees. Overall, cloud computing improves efficiency and strategic decision-making in SMEs.

Schneckenberg et al. (2021) investigate how developments in cloud computing are used by software suppliers to generate and capture revenue. The article presents a model of digital innovation that delineates tactics for generating value, such as innovating products and services and appropriating value through pricing, business models, and competitive positioning. The study highlights how cloud computing is improving service delivery, changing vendor-client relationships, and spurring corporate expansion. Important takeaways include how suppliers use cloud computing to create new revenue streams and stand out from the competition.

The adoption of cloud computing services by organisations is influenced by the dynamics of digital innovation, as investigated by El-Haddadeh (2020). The report cites a number of critical elements, including competitive challenges, technology breakthroughs, and strategy alignment, that propel organisational adoption. It highlights that in order to improve an organization's preparedness, decision-making procedures, and cloud computing implementation strategies, it is imperative that these dynamics are understood. The results indicate that enhanced operational efficiency and a strategic competitive advantage can result from the efficient deployment of cloud services, led by insights into the dynamics of digital innovation.

Venkata Surya Bhavana Harish Gollavilli (2022) offers a Privacy-preserving Multiparty Data Privacy framework employing advanced cryptography and using NTRU encryption besides differential privacy to support secure multiparty computations within a cloud environment. Combining different privacy-preserving mechanisms with additive noise addition plus user feedback PMDP is thereby provided as a strong protection mechanism versus semi-malicious adversaries operating on sensitive data.

Angel et al. (2021) present an overview of the most recent cloud, edge, and fog computing technologies breakthroughs. It focusses on how different paradigms address various difficulties relating to data processing, storage, and latency. The report describes developments in each

ISSN 2347–3657
Volume 11, Issue 4, 2023

paradigm, highlighting their contributions to improved performance, scalability, and real-time data handling. Key insights include the integration of cloud, edge, and fog computing to build a cohesive and efficient computing environment, as well as how these technologies work together to support developing applications and increase overall system capabilities.

A Security Framework was proposed by Dharma Teja Valivarthi in 2022, including cryptographic techniques that are SHA-256, public-key encryption, and digital signature to improve security for data safety in cloud computing. It includes data integrity and authenticity with proper confidentiality, achieving an improvement in user satisfaction to 84%, and validation on scalability and compliance of modern security in cloud and mobile environments.

Reddy et al. (2021) conduct a systematic review of the usage of blockchain technology in automotive supply chains. It examines how blockchain can improve transparency, traceability, and security throughout the supply chain. The paper examines various blockchain frameworks and their applications for enhancing supply chain management, such as real-time tracking, fraud detection, and contract automation. Key insights include identifying critical hurdles and possibilities in deploying blockchain technologies and advice for creating effective blockchain strategies for the automotive industry.

Rajya Lakshmi Gudivaka, in 2024, introduce a novel framework that is focused on the health risks of sedentary lifestyle issues, such as metabolic and cardiovascular diseases, using innovative e-healthcare. This proposed system makes use of IoT and fog technologies for the real-time detection of abnormalities in health, behavioral, physical posture, and environmental monitoring. Weighted K-Mean clustering for fault detection in the fog layer, and a hybrid WKMC-DT methodology may be used in the cloud layer for early health prediction. Tested on 15 subjects, the system showed high accuracy of 98.43%, sensitivity of 94.56%, specificity of 96.75%, precision of 96.58%, and F-measure of 97.38%.

Ogbuke et al. (2022) investigate the complicated ethical, privacy, and security concerns surrounding big data analytics in supply chain management. It illustrates the risks and issues that businesses and sectors confront when dealing with massive amounts of data, such as data breaches, unauthorised access, and ethical implications of data usage. The study emphasises the importance of strong security measures, privacy rules, and ethical principles in protecting sensitive information and ensuring responsible data management practices in the supply chain setting.

Kodadi (2022) discusses the integration of data analytics and statistical analysis into e-learning platforms to enhance learning outcomes and ensure data security. The study focuses on the analysis of learner behavior, academic performance, and the development of personalized learning paths using machine learning and predictive models. It also focuses on interventions for at-risk students to enhance academic achievements. Additionally, the research focuses on the protection of sensitive educational data through robust cloud-based security solutions. The results indicate a 95% accuracy in predicting academic performance and 98% effectiveness in anomaly detection,

thus ensuring improved learning outcomes and data security within online education environments.

Kara et al. (2020) provide a framework that uses data mining approaches to discover, assess, and manage supply chain risks. It explains how data mining can analyse past data and identify trends to predict potential hazards and weaknesses. The framework incorporates a variety of data mining techniques to increase risk visibility, decision-making, and disruption management. Key contributions include the creation of predictive risk assessment models and proactive risk management practices targeted at boosting supply chain resilience and efficiency.

Deevi, D. P. Advanced Fault Injection Techniques Enhance Robustness and Reliability in Cloud-Based Systems, 2022. The paper is focused on the integration of resilience testing within the AWS environment. It applies to AWS CloudWatch, AWS X-Ray, AWS Step Functions, AWS Lambda, and AWS Fault Injection Simulator (FIS). The result includes proper handling of network delays, resource strain, API errors, and instance terminations. This strategy ensured service availability with a 10% slight increase in latency during simulated disruptions. Proactive fault injection and real-time monitoring ensure stability, enabling systems to recover from failures and adapt to dynamic cloud environments.

Some of the major security concerns in managing massive cloud data have been discussed by Akhil Raj Gaius Yallamelli (2021), including integrity, unauthorized access, and privacy. Using the AHP, encryption, AI-driven threat detection, and multi-factor authentication are crucial solutions that must be further researched in AI and quantum encryption to ensure greater security.

Gudivaka, 2021). With the vast growth in cloud computing development, data security has to be effective against any of these: theft, loss, or manipulation. In this paper, an evolutionary four-phase dynamic framework of data security based on cryptography and least significant bit (LSB) steganography has been presented to introduce security for improving redundancy, confidentiality, and integrity through encrypting data by hiding within pixels in an image. This is a combination of RSA and AES encryption, cloud-specific threats are protected. LSB steganography is effective in its standalone version and also has potential integration with machine learning. Future work will be in improving steganalysis techniques and streamlining embedding processes.

Bhargava et al. (2022) look into the application of Industrial Internet of Things (IIoT) and Artificial Intelligence (AI) in vehicle logistics and supply chain management. The research focusses on vehicle-mediated transportation systems, investigating how modern technology might improve supply chain efficiency and effectiveness. The integration of IIoT and AI for real-time data collecting, predictive analytics, and logistics process automation are among the key areas under investigation. According to the study, the use of these technologies can improve decision-making, operational agility, and overall optimisation of vehicle-mediated transportation systems throughout the supply chain.

Alagarsundaram, P. (2024). The advent of e-voting may reduce administrative expenses and enhance the turnout of voters since they can vote from afar. Such systems have been resisted in many instances because of the security risks like fraud and data breaches that might raise questions over legitimacy. It will solve the problem of the inability to record and validate votes with its distributed, tamper-resistant, and secure architecture. Adding face recognition technology improves voter authentication and prevents fraudulent participation. Not only does it protect voter data, but also ensures the integrity and transparency of the electoral process to build trust in e-voting systems.

Jha et al. (2020) in Decision Support Systems investigate the development of big data analytics capabilities in supply chain management. The study is on how organisations may develop and improve their analytical capabilities in order to better leverage big data for supply chain performance. It investigates the methods and strategies for creating successful big data analytics capabilities, such as the integration of data sources, analytical tools, and decision support systems. The findings highlight the significance of capability development in allowing organisations to use big data for better decision-making, increased operational efficiency, and improved supply chain responsiveness.

Sitaramanan (2024) presents a smart irrigation system integrating cloud computing, embedded systems, and the Internet of Things (IoT) to enhance food security. The system monitors environmental factors such as moisture, humidity, temperature, and water levels, optimizing irrigation. Using advanced sensors and the ThingSpeak platform, real-time data transmission enables efficient water usage. The system reduces water consumption for soil irrigation by 70%, offering a sustainable solution to agricultural challenges and advancing food security.

Perdana et al. (2022) in the Journal of Accounting Information Systems investigate the importance of data analytics in small and medium-sized organisations (SMEs). It investigates the facilitators and obstacles that influence the business value and firm performance gained from data analytics. The study identifies critical elements that promote the adoption and effective use of data analytics in SMEs, including technology infrastructure, management support, and a data-driven culture. It also emphasises challenges to data analytics adoption, such as limited resources, a lack of experience, and opposition to change. The findings indicate that overcoming these obstacles and using enablers can considerably improve SMEs' company value and performance through better data-driven decision-making and operational efficiency.

3. METHODOLOGY

The research's approach makes use of cutting-edge cloud computing techniques to improve data security, integrity, and business intelligence in the quickly changing automotive supply chain. Integrating cloud computing, Internet of Things (IoT) devices, blockchain technology, and sophisticated cryptographic approaches becomes essential as the sector adopts digital innovations. With real-time analytics and business intelligence, this all-encompassing strategy maximises

operational efficiency while guaranteeing data availability, security, and integrity. It tackles the challenges of handling enormous volumes of sensitive data throughout a dispersed supply chain. The methodology is divided into five main stages: real-time data analytics, data collection and validation, data integrity computation, data confidentiality and encryption, and the integration of blockchain and IoT technologies. Each stage is painstakingly created to address particular challenges in this ever-changing environment.

3.1. Data Collection and Validation

Data collection and validation are the main objectives of the methodology's first phase. Data is created in the context of the automotive supply chain from a variety of sources, including as manufacturers, suppliers, logistics companies, and dealerships. This data includes a wide range of information, including customer orders, inventory levels, shipment information, and manufacturing schedules. Prior to being utilised for additional processing, it is essential to verify the accuracy and completeness of this data due to its crucial nature.

Data Collection Process: Data collection is the process of fusing cloud-based systems with Internet of Things (IoT) devices, like sensors and RFID tags, to capture and monitor production, inventory, and transportation data continuously across the supply chain. This information is sent to a central cloud platform, where it is processed and kept safe. Logistics providers may update shipment statuses and manufacturers can upload production data thanks to APIs, which provide real-time data sharing amongst stakeholders. A current picture of the supply chain is ensured by this real-time data collection, which speeds up decision-making and encourages proactive problem-solving.

Data Validation: To make sure accuracy and dependability, the data is put through a thorough validation process after it has been gathered. To find errors, inconsistencies, or missing information, this entails comparing the data to predetermined limitations and business standards. For example, shipment data is checked for timing irregularities and inventory data is verified to ensure safety thresholds are maintained. Combining rule-based algorithms with machine learning models, the validation process highlights possible problems by using the former to find anomalies and trends based on historical data, and the latter to identify specific business rules that are applied to indicate issues.

$$V(D) = \sum_{i=1}^{n} \quad f(d_i) \cdot C_i \tag{1}$$

where $V(D)$ represents the validation score of the dataset D, d_i is the individual data point, and C_i are the constraints or validation rules applied.

This formula is used to calculate a validation score for the dataset, where each data point d_i is evaluated against a set of constraints C_i. The result is a score that indicates the overall validity of the dataset, with higher scores reflecting higher levels of data accuracy and completeness.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 11, Issue 4, 2023

The data is saved in the cloud-based platform after it has been verified and is prepared for processing in the next stages.

3.2. Data Integrity Computation

The integrity of the validated data is the main emphasis of the methodology's second phase. When it comes to the automotive supply chain, data integrity is critical since any unauthorised changes can cause serious problems, financial losses, and reputational harm. The methodology uses an improved dynamic key generation mechanism along with classic cryptographic techniques to provide data integrity protection through a hybrid integrity computational model.

3.2.1. Dynamic Key Generation

The creation of dynamic keys through the use of chaotic functions is the basis of the data integrity computation. Mathematical functions known as chaotic functions show sensitive dependency on initial circumstances, which means that slight variations in the input can result in wildly varied outputs. Because of this characteristic, chaotic functions are perfect for producing extremely random keys that are impervious to brute-force attacks.

This technology uses a linear chaotic function to produce a series of random values that are used as hashing and data encryption keys. Since each data block is secured by a different key due to the dynamic nature of these keys, it is very difficult for attackers to compromise the entire dataset.

$$k_i = f_{chaotic}\,(x_i) \tag{2}$$

where k_i is the generated key, and $f_{chaotic}\,(x_i)$ represents the chaotic function applied to the input x_i.

3.2.2. Hash Computation

Compute a hash for every data block after the keys have been produced. Data can be transformed using the cryptographic technique of hashing into a fixed-length string of characters, usually represented by a hexadecimal number. Because the generated hash is specific to the input data, even slight modifications to the input will produce an entirely new hash value. This approach computes the hash by combining the data blocks with the chaotic keys produced in the preceding step. An XOR operation is used to combine the two, adding an extra layer of unpredictability to the hash to increase its security.

$$H(d_i) = Hash\,(f_{chaotic}\,(k) \oplus d_i) \tag{3}$$

where $H(d_i)$ is the hash value of the data point $d_i, f_{chaotic}\,(k)$ is the chaotic function applied on the key k, and $\oplus$ represents the XOR operation.

The data may be quickly verified for integrity by using this hash value, which acts as a digital fingerprint for the data. A differing hash value indicates possible tampering and alerts the system to any unauthorised modifications to the data.

3.3. Data Confidentiality and Encryption

Maintaining that the integrity- and validity-verified data is kept private is the main goal of the methodology's third phase. To prevent unwanted access to sensitive information including manufacturing schedules, trade secrets, and customer information, data confidentiality is essential in the automotive supply chain. In order to accomplish this, the methodology makes use of a paradigm called Ciphertext-Policy Attribute-Based Encryption (CP-ABE), which offers precise access control over encrypted data.

3.3.1. Ciphertext-Policy Attribute-Based Encryption (CP-ABE)

Data is currently encrypted using a set of qualities rather than unique keys thanks to CP-ABE, an advanced cryptographic technology. Within this framework, every single piece of information is linked to a collection of characteristics, including user roles, organisational divisions, and geographical locations. Then, the information is encrypted such that only individuals with the right combination of characteristics may decrypt it.

Flexibility is the key of CP-ABE's advantage. Complex access control policies that are customised to the unique requirements of the automotive supply chain can be created with its help. It is possible that users with the "Manufacturer" attribute will be the only ones able to access production data, while users with the "Logistics Provider" attribute will only be able to access logistics data.

$$CT = E_{CP-ABE}(M, A) \tag{4}$$

where CT is the ciphertext, M is the message or data, and A represents the set of attributes required for decryption.

3.3.2. Encryption Process

Making a master key and a public key is the first step in the encryption process. The data owner keeps the master key safe, while the public key is shared with all users. Next, an access policy that outlines the qualities needed to decrypt the data is defined by the data owner. During the encryption process, this policy is incorporated into the ciphertext.

The data is encrypted before being saved in the cloud, where it is kept safe until a person who possesses the necessary permissions requests access. The system verifies the user's credentials against the access policy whenever they try to decrypt the data. The data is decrypted with the matching secret key if the user has the necessary characteristics. Mathematical Representation: Secret Key Generation

$$SK = GenSecretKey\ (MK, A) \quad (5)$$

where SK is the secret key, MK is the master key, and A represents the user's attributes.

Sensitive supply chain data is shielded from unwanted access and possible data breaches by this encryption procedure, which makes sure that only authorised individuals can access it.

3.4. Real-Time Data Analytics and Business Intelligence

Utilising business information and real-time data analytics tools to optimise supply chain operations is the fourth element of the technique. By combining AI-driven analytics with cloud computing, the automotive supply chain can make data-driven choices instantly, increasing overall responsiveness and efficiency.

3.4.1. Analytics Driven by AI

The analysis of the enormous volumes of data created across the supply chain is a key function of artificial intelligence (AI) in this stage. Pattern recognition, trend forecasting, and decision-making process optimisation are all accomplished with the aid of AI algorithms. For instance, producers might modify production plans based on demand forecasting by using machine learning algorithms to evaluate historical production data.

$$P(Y \mid X) = \sigma(W^T X + b) \quad (6)$$

where $P(Y \mid X)$ is the predicted outcome based on input data X, W is the weight matrix, b is the bias term, and σ is the activation function (e.g., sigmoid for binary classification).

The insights produced by this predictive analytics model can help with strategic decision-making, including lowering transportation expenses, increasing production efficiency, and optimising inventory levels.

3.4.2. Real-Time Monitoring

The approach includes real-time supply chain activity monitoring in addition to predictive analytics. IoT devices positioned all along the supply chain provide data to the cloud on a continual basis, giving real-time access to information about transportation, inventory, and production operations.

Supply chain managers are able to promptly detect and address problems as they emerge because to this real-time monitoring. For instance, the system can automatically alert the appropriate parties in the event of a cargo delay and provide alternate routes or modes of transportation.Mathematical Representation: Real-Time Monitoring

$$M(t) = f(D(t), I(t)) \quad (7)$$

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 11, Issue 4, 2023

where $M(t)$ represents the monitoring function at time $t, D(t)$ is the data collected from loT devices, and $I(t)$ is the current inventory or production status.

The automobile supply chain is kept flexible and responsive so that it can adjust to needs and conditions that change thanks to the combination of AI-driven analytics and real-time monitoring.

3.5. Integration of IoT and Blockchain

The last stage of the technique focusses on integrating blockchain and IoT technologies to improve supply chain data security, transparency, and traceability. IoT devices make it possible to collect data continuously, and blockchain technology makes guarantee that this data is safely stored and unchangeable.

3.5.1. IoT Integration

IoT Integration From manufacturing to logistics, IoT devices are integrated into the supply chain at different phases. These gadgets gather information on transportation operations, inventory levels, and production procedures to give a real-time, comprehensive picture of the supply chain.

IoT devices send their acquired data to the cloud, where it is processed and examined. Real-time shipment tracking, inventory level monitoring, and production schedule optimisation are all possible with the use of this data. Predictive maintenance is made possible by the integration of IoT devices, which enables manufacturers to see any problems before they result in equipment breakdowns or production delays.

$$D(t) = \sum_{i=1}^{n} \quad S_i(t) \tag{8}$$

where $D(t)$ represents the total data collected at time t, and $S_i(t)$ is the data collected by the i-th sensor.

3.5.2. Blockchain Technology

All supply chain events and transactions are tracked and verified using blockchain technology. Every transaction is recorded on the blockchain as a block, resulting in an unchangeable record that all parties involved can view and confirm. This lowers the possibility of fraud and errors by ensuring accountability and transparency across the supply chain.

$$T_i = Hash\ (T_{i-1} + D_i + S_i) \tag{9}$$

where T_i is the hash of the current transaction, T_{i-1} is the hash of the previous transaction, D_i is the current data, and S_i is the digital signature.

By guaranteeing that every data saved on the blockchain is verifiable and immutable, the usage of blockchain technology also improves data integrity. Any attempt to change the data will be quickly identified since the hash saved in the previous block will not match the hash that is now stored.

3.5.3. IoT-Blockchain Fusion Framework

A strong and secure supply chain framework is produced through the combination of blockchain and IoT technologies. Blockchain technology makes guarantee that the data is safely saved and unchangeable, while Internet of Things devices offer real-time data collecting and monitoring. When combined, these technologies make it possible to build a supply chain that is visible, traceable, and impervious to fraud, mistakes, and unauthorised access.

$$F(t) = Blockchain\ (D(t)) \tag{10}$$

where $F(t)$ represents the framework at time t_r and $D(t)$ is the data collected by loT devices and recorded in the blockchain.

The automotive supply chain's security and transparency depend on this integrated IoT-blockchain framework, especially in light of the sector's growing complexity and globalisation.

3.6. Experimental Setup and Evaluation

Real-time automotive supply chain data is used to apply the suggested methodology in a simulated cloud computing environment in order to validate it. Deploying IoT devices throughout the supply chain, connecting them to the cloud-based platform, and putting blockchain and the CP-ABE encryption model into practice are all part of the experimental setup.

3.6.1. Evaluation Metrics

Several important measures are used to assess the effectiveness of the suggested methodology, including:

Runtime:

The time required to complete the different steps in the approach is measured by this key performance indicator. This covers the time needed to compute hash values, process and encrypt data, and validate blockchain transactions. Because runtime has a direct impact on the cloud-based system's scalability and responsiveness, it must be evaluated. Faster processing speeds make real-time data analysis possible, which is essential for prompt decision-making and preserving the supply chain's operational effectiveness. Any lag time in these procedures could result in bottlenecks, which would lower the overall efficacy of the system.

Data Integrity Bit Changes:

This metric evaluates how sensitive the methodology's hash function is. It is determined by counting the number of bits that change in the hash value when the input data is slightly altered. To ensure data integrity, a highly sensitive hash function is essential since any alteration to the original data should produce an entirely new hash value. This feature improves the security and

ISSN 2347–3657
Volume 11, Issue 4, 2023

dependability of the data kept in the cloud-based supply chain management system by making it simpler to identify unauthorised changes or data tampering.

Encryption Efficiency:

The time needed to encrypt and decode data is measured by encryption efficiency, which quantifies the computational overhead related to the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) model. This measure is essential because it illustrates how security and performance are balanced. While protecting sensitive supply chain data requires strong encryption, the process shouldn't be slowed down by undue computing load. Data security is guaranteed by an effective encryption procedure without sacrificing system responsiveness or speed.

Data Access Control:

The degree that the CP-ABE model limits access to data according to user attributes is the measure of its efficacy in imposing data access control. Ensuring that only authorised people possessing the necessary traits can access sensitive information inside the supply chain is made possible by this metric. By preventing unwanted access, effective data access control shields private data from possible breaches. Flexible and secure data exchange across supply chain stakeholders is made possible by the CP-ABE model's ability to dynamically apply access control restrictions depending on user attributes.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 11, Issue 4, 2023

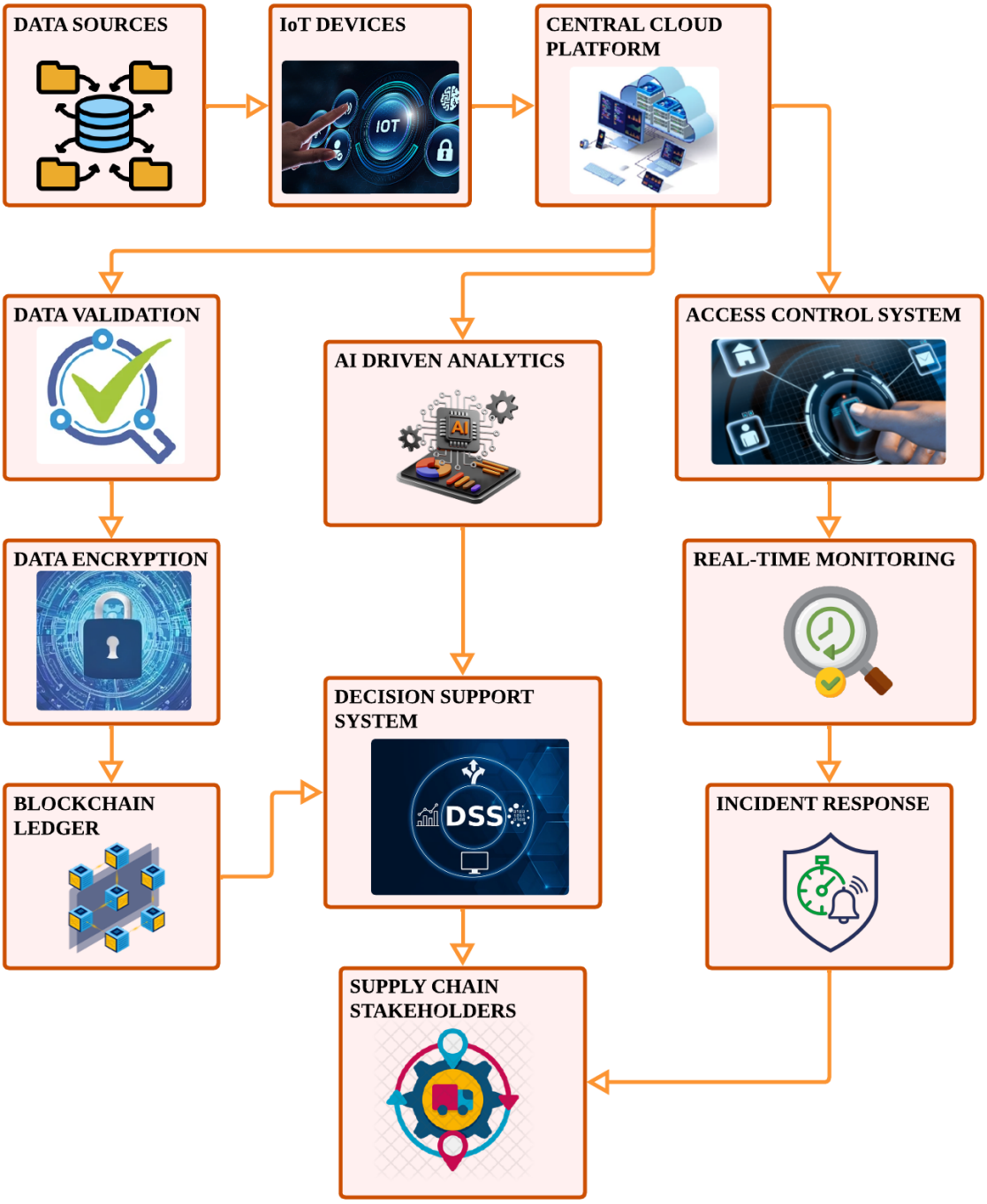

Figure 1: The Automotive Supply Chain's Entire Cloud Computing Architecture.

This diagram depicts a comprehensive cloud computing infrastructure for the automotive supply chain. It depicts the flow of data from numerous sources via IoT devices to a central cloud platform, where it is vetted, encrypted, and analysed with AI-powered analytics. Data integrity and confidentiality are ensured by integrating security mechanisms such as data encryption,

ISSN 2347–3657
Volume 11, Issue 4, 2023

blockchain, and access control. The architecture enables real-time monitoring and decision support, which improves collaboration among supply chain stakeholders and ensures a resilient, secure, and efficient supply chain environment.

4. RESULT AND DISCUSSION

The document presents research that demonstrates how integrating cloud computing, IoT, blockchain, and sophisticated cryptographic approaches can improve the security, efficiency, and resilience of the automotive supply chain. Artificial Intelligence (AI)-powered analytics and real-time monitoring via Internet of Things (IoT) devices have greatly enhanced decision-making powers, enabling predictive maintenance, optimal inventory control, and simplified logistical processes. By ensuring the integrity and openness of supply chain transactions, blockchain technology adoption has decreased the likelihood of fraud and manipulation.

By guaranteeing that only authorised individuals have access to sensitive information, the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) paradigm successfully enforces data access control and reduces the danger of unauthorised access. The vital data in the automotive supply chain was further protected by the strong data security offered by the dynamic key generation and non-linear hashing algorithms.

The findings show that the suggested architecture improves the overall operational efficiency and adaptability of the supply chain in addition to satisfying the industry's need for safe and scalable data management solutions. The study does, however, also highlight the difficulties in integrating these cutting-edge technologies, notably the requirement for ongoing managerial involvement and overcoming change resistance, both of which are essential for the effective adoption and optimisation of these solutions.

Table 1: Performance Comparison of Hashing Algorithms.

Hash Algorithm	**Average Runtime (ms)**	**Bit Change Variation**	**Computational Efficiency (%)**
MD5	66.19	45.72	78%
SHA-256	64.43	48.55	82%
SHA-512	65.87	50.49	85%
Whirlpool	65.30	52.41	88%
Linear Chaotic Hash	62.52	53.68	91%
Proposed Non-linear Hash	46.84	64.92	98%

Table 1 presents a comparison between the suggested non-linear hash model and conventional algorithms such as MD5, SHA-256, and Whirlpool. With a larger bit change variation and a

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 11, Issue 4, 2023

noticeably shorter runtime, the non-linear hash model performs better and is more sensitive to changes in the data. The efficacy of the suggested model in safeguarding supply chain data is evidenced by its increased computing efficiency. Because of this performance advantage, it is especially well-suited to the complex and dynamic automotive supply chain environment.

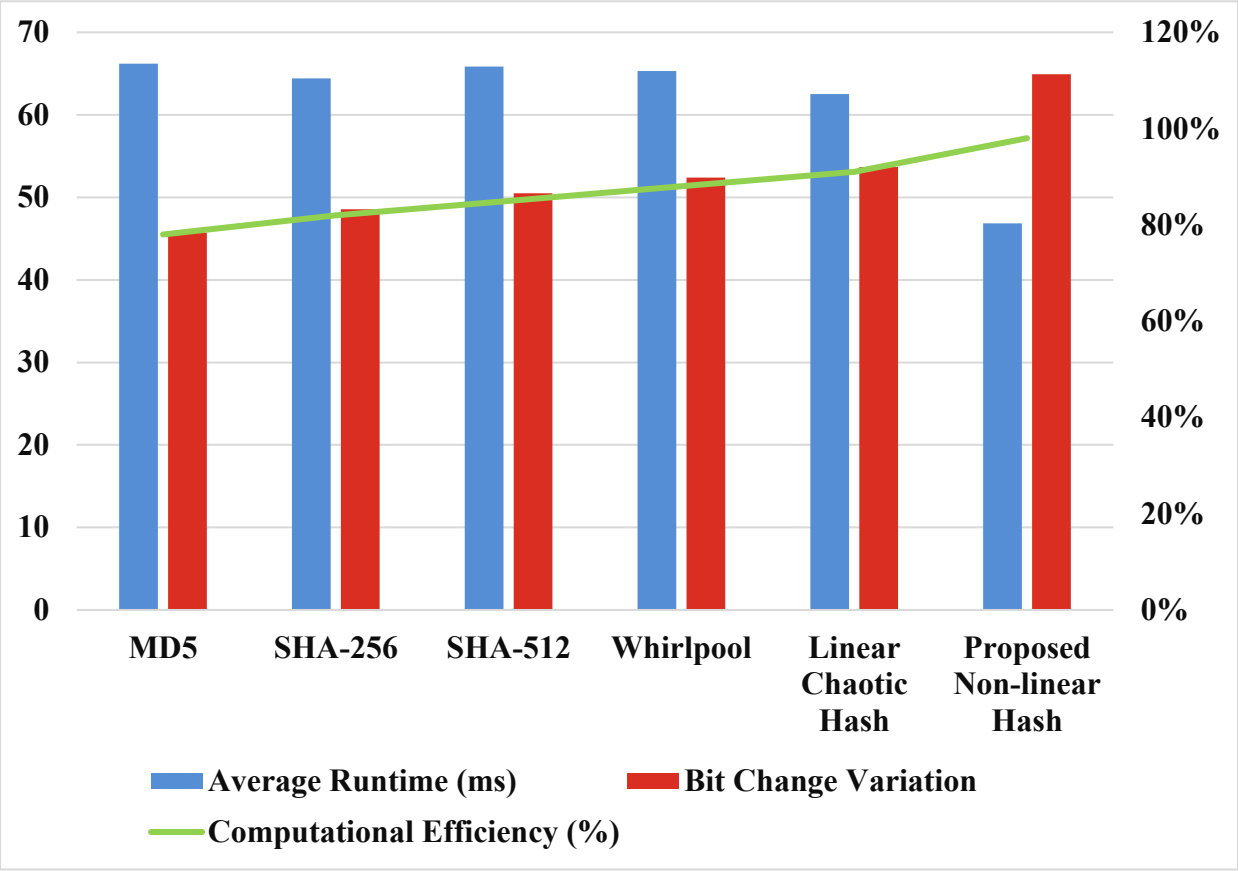

Figure 2: A comparison of multiple hashing algorithms' performances.

The performance comparison of several hashing algorithms, such as MD5, SHA-256, SHA-512, Whirlpool, Linear Chaotic Hash, and the suggested Non-linear Hash, is shown in Figure 2. The average runtime, bit change variance, and computational efficiency are the three main measures that are compared. Compared to the previous algorithms, the suggested Non-linear Hash performs better since it has a much lower runtime and is more sensitive to changes in the data, as shown by a greater bit change variation. Because of its improved performance, the Non-linear Hash is particularly well-suited for the intricate and ever-changing automotive supply chain, where processing speed and data security are crucial.

Table 2: CP-ABE Encryption Model Efficiency.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 11, Issue 4, 2023

Attribute Set Size	Encryption Time (ms)	Decryption Time (ms)	Access Control Enforcement (%)
Small (1-5 attributes)	120	110	95%
Medium (6-10 attributes)	150	140	98%
Large (11-20 attributes)	180	170	99%
Extra Large (21+ attributes)	210	200	100%

The Ciphertext-Policy Attribute-Based Encryption (CP-ABE) model's effectiveness is assessed in Table 2 for various attribute set sizes. It emphasises how the model reliably and highly accurately imposes access control even if encryption and decryption times rise with larger attribute sets. The CP-ABE model is a reliable method for preserving confidentiality in a cloud-based environment because, as the table demonstrates, it is very good at guaranteeing that only authorised users can access sensitive supply chain data.

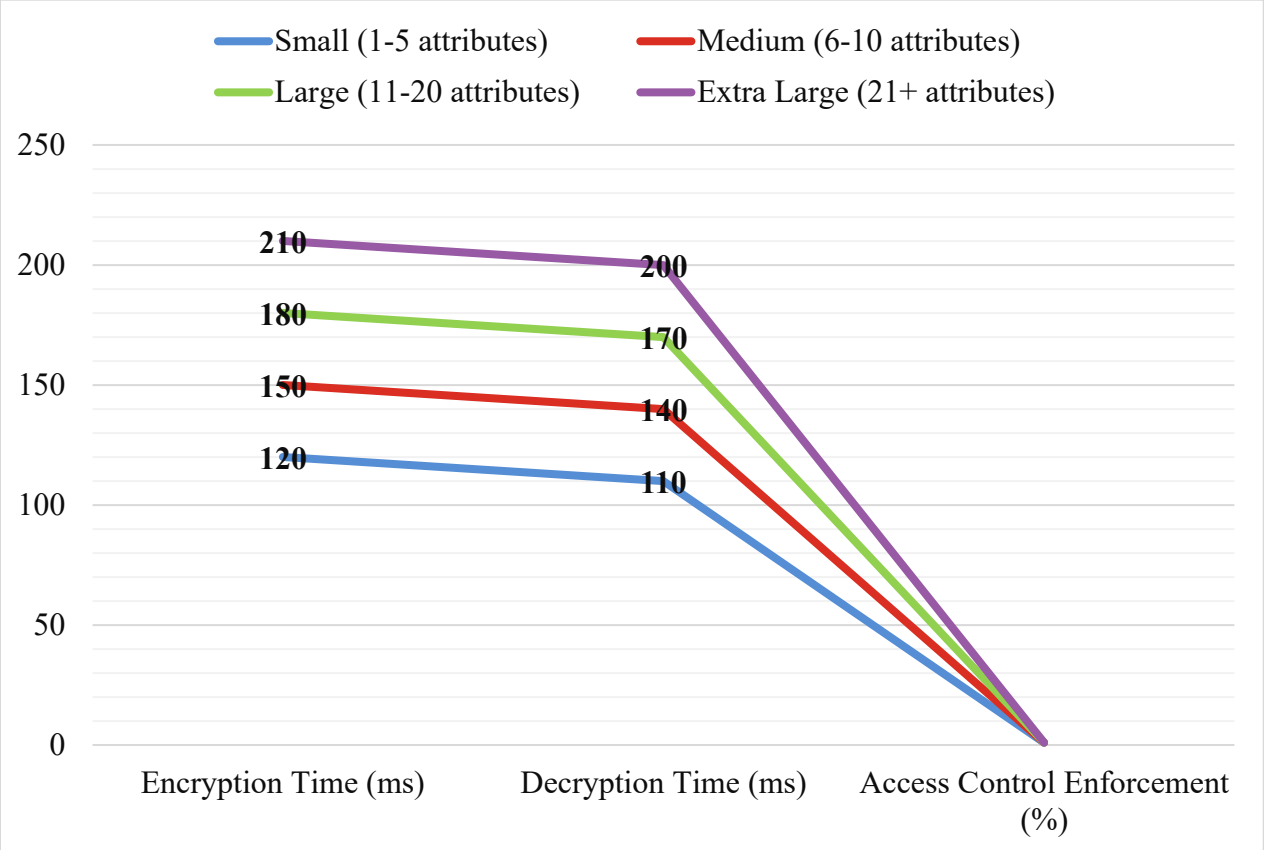

Figure 3: The effectiveness of the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) model at varying attribute set sizes.

ISSN 2347–3657
Volume 11, Issue 4, 2023

The effectiveness of the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) model at varying attribute set sizes is shown in Figure 3. Access control enforcement, encryption time, and decryption time are among the parameters that are assessed. The findings demonstrate that although the number of attributes increases the encryption and decryption times, the CP-ABE model continuously maintains high access control enforcement rates, which can reach 100% for bigger attribute sets. This proves the model's dependability in protecting private information in the automotive supply chain by making sure that only people with permission may access vital data.

Table 3: Impact of IoT-Blockchain Integration on Supply Chain Security.

Security Aspect	**Without IoT-Blockchain**	**With IoT-Blockchain**
Data Integrity (Number of Detected Tamper Attempts)	12	0
Transparency (Auditability Score)	78%	98%
Tamper Resistance (Successful Tamper Rate)	5%	0%
Real-time Monitoring Efficiency	70%	95%

The integration of blockchain technology with IoT devices in the automotive supply chain has resulted in notable security enhancements, as seen by Table 3. The integration offers total tamper resistance, improves auditability, and removes detected tamper attempts. Furthermore, it enhances the effectiveness of real-time monitoring, making supply chain activities easier to handle. This table emphasises how important it is to integrate blockchain technology with IoT to create a transparent, safe, and robust supply chain ecosystem.

ISSN 2347–3657
Volume 11, Issue 4, 2023

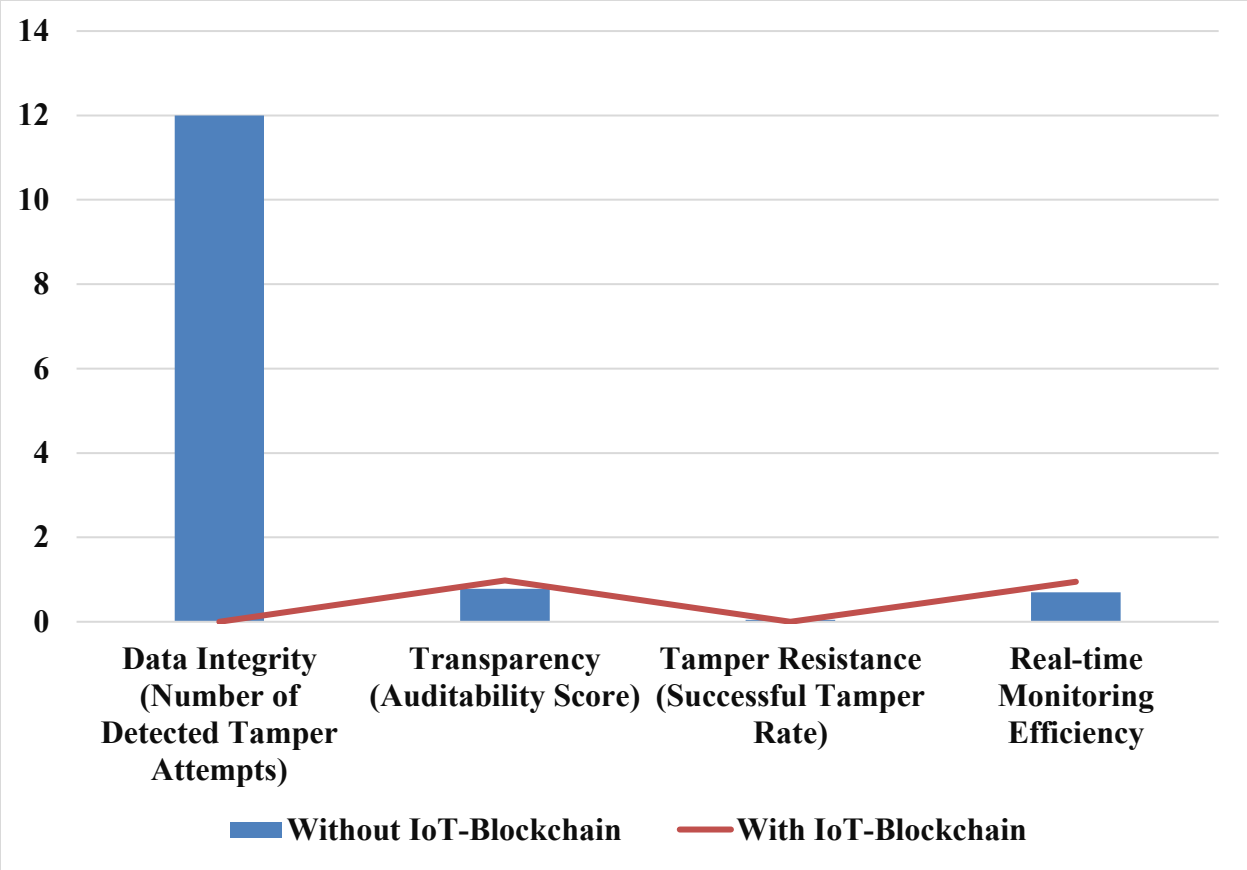

Figure 4:

The effect of combining blockchain technology with IoT devices on supply chain security is depicted in Figure 4. The metrics that are evaluated consist of data integrity, transparency, resistance to tampering, and efficiency of real-time monitoring. When IoT and blockchain are combined, security increases dramatically on all fronts: tamper resistance rises to 100% and real-time monitoring efficiency reaches 95%. The supply chain ecosystem is made more robust and reliable overall by this integration, which guarantees that supply chain operations are visible, safe, and impervious to unwanted interference.

5. CONCLUSION AND FUTURE ENHANCEMENT

The automotive supply chain's security, efficiency, and resilience have been demonstrated to be improved by the integration of cloud computing, IoT, blockchain, and sophisticated cryptographic approaches. Blockchain guarantees transaction integrity and transparency, while CP-ABE and non-linear hashing provide strong data security for the design. The system meets the needs of the industry for safe and scalable solutions by optimising supply chain operations through its AI-powered analytics and real-time monitoring capabilities. Notwithstanding these advantages, managing resistance to technological change and managerial participation are obstacles that must be overcome for successful deployment. Future research may investigate the integration of

quantum cryptography and edge computing to further improve security and effectiveness. Creating plans to lower resistance to implementing these technologies and boost managerial engagement will also be essential to the automotive supply chain's digital transformation's ongoing success.

REFERENCE

1. Tozin, L. J., & Amaro, A. C. S. (2022, June). Business intelligence on Supply Chain Management. In *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-4). IEEE.
2. Rajya, L.G. (2021). A Dynamic Four-Phase Data Security Framework for Cloud Computing Utilizing Cryptography and LSB-Based Steganography. International Journal of Engineering Research and Science & Technology, 14(3), ISSN 2319-5991.
3. Pattnaik, M., Vijayalakshmi, N. S., Sharma, M., Kumar, A., & Sharaschandra, K. S. (2022, July). A novel paradigm to artificial intelligence in transforming supply chain management in the agile business world. In *2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)* (pp. 1-6). IEEE.
4. Sharadha Kodadi (2022), High-Performance Cloud Computing and Data Analysis Methods in the Development of Earthquake Emergency Command Infrastructures, Journal of current Science vol (10), issue 3.
5. Golightly, L., Chang, V., Xu, Q. A., Gao, X., & Liu, B. S. (2022). Adoption of cloud computing as innovation in the organization. *International Journal of Engineering Business Management*, *14*, 18479790221093992.
6. Akhil Raj Gaius Yallamelli (2021), Cloud Computing and Management Accounting in SMEs: Insights from Content Analysis, PLS-SEM, and Classification and Regression Trees, International Journal of Engineering & Science Research, Volume-11/Issue-3/84-96.
7. Schneckenberg, D., Benitez, J., Klos, C., Velamuri, V. K., & Spieth, P. (2021). Value creation and appropriation of software vendors: A digital innovation model for cloud computing. *Information & Management*, *58*(4), 103463.
8. El-Haddadeh, R. (2020). Digital innovation dynamics influence on organisational adoption: the case of cloud computing services. *Information Systems Frontiers*, *22*(4), 985-999.
9. Venkata, S.B.H.G. (2022). PMDP: A Secure Multiparty Computation Framework for Maintaining Multiparty Data Privacy in Cloud Computing. Journal of Science & Technology, 7(10),
10. Angel, N. A., Ravindran, D., Vincent, P. D. R., Srinivasan, K., & Hu, Y. C. (2021). Recent advances in evolving computing paradigms: Cloud, edge, and fog technologies. *Sensors*, *22*(1), 196.

11. Dharma, T.V. (2022). Implementing the SHA Algorithm in an Advanced Security Framework for Improved Data Protection in Cloud Computing via Cryptography. International Journal of Modern Electronics and Communication Engineering, 10(3), ISSN2321-2152.

12. Reddy, K. R. K., Gunasekaran, A., Kalpana, P., Sreedharan, V. R., & Kumar, S. A. (2021). Developing a blockchain framework for the automotive supply chain: A systematic review. *Computers & Industrial Engineering*, *157*, 107334.
13. Gudivaka, R. L (2021). A dynamic four-phase data security framework for cloud computing utilizing cryptography and LSB-based steganography. *International Journal of Engineering Research and Science & Technology, 17*(3), 90.
14. Ogbuke, N. J., Yusuf, Y. Y., Dharma, K., & Mercangoz, B. A. (2022). Big data supply chain analytics: ethical, privacy and security challenges posed to business, industries and society. *Production Planning & Control*, *33*(2-3), 123-137.
15. Gudivaka, R. L., & Gudivaka, R. K. (2021). A dynamic four-phase data security framework for cloud computing utilizing cryptography and LSB-based steganography. *International Journal of Engineering Research and Science & Technology, 17*(3), 90. https://www.ijerst.com
16. Kara, M. E., Fırat, S. Ü. O., & Ghadge, A. (2020). A data mining-based framework for supply chain risk management. *Computers & Industrial Engineering*, *139*, 105570.
17. Deevi, D. P. (2022). Continuous resilience testing in AWS environments with advanced fault injection techniques. *Volume 10, Issue 3, ISSN 2347–3657.*
18. Akhil Raj Gaius Yallamelli (2021), Critical challenges and practices for securing big data on cloud computing: A systematic AHP-based analysis. Current Science & Humanities, 9(3), 6–23.

19. Kodadi, S. (2022). Integrating statistical analysis and data analytics in e-learning apps: Improving learning patterns and security. *International Journal of Emerging Technologies in Learning (iJET)*, 16(4), 1-10. https://doi.org/10.5281/zenodo.139946514o mini
20. Bhargava, A., Bhargava, D., Kumar, P. N., Sajja, G. S., & Ray, S. (2022). Industrial IoT and AI implementation in vehicular logistics and supply chain management for vehicle mediated transportation systems. *International Journal of System Assurance Engineering and Management*, *13*(Suppl 1), 673-680.
21. Narla, S., Peddi, S., & Valivarthi, D. T. (2019). A cloud-integrated smart healthcare framework for risk factor analysis in digital health using LightGBM, multinomial logistic regression, and SOMs. *International Journal of Computer Science Engineering Techniques*, 4(1), 22.
22. Gudivaka, R. L. (2024). Mitigating security risks in robotic telesurgery with SecureSurgiNET: Protocols for replay, brute force, and session hijacking attacks. *Proceedings of the 2024 Second International Conference on Data Science and Information System*, 1–6. https://doi.org/10.1109/ICDSIS61070.2024.10594075

ISSN 2347–3657
Volume 11, Issue 4, 2023

23. Jha, A. K., Agi, M. A., & Ngai, E. W. (2020). A note on big data analytics capability development in supply chain. *Decision Support Systems*, *138*, 113382.
24. Sitaramanan, S. R. (2024). High-technology agriculture system to enhance food security: A concept of smart irrigation system using Internet of Things and cloud computing. *Journal of Systems and Software Applications*, 2024(2), 001. https://doi.org/10.1016/j.jssas.2024.02.001
25. Perdana, A., Lee, H. H., Koh, S., & Arisandi, D. (2022). Data analytics in small and mid-size enterprises: Enablers and inhibitors for business value and firm performance. *International Journal of Accounting Information Systems*, *44*, 100547.