




Review

# Challenges, Issues, and Recommendations for Blockchain- and Cloud-Based Automotive Insurance Systems

Abdul Mateen <sup>1,2,†</sup>, Adia Khalid <sup>3,†</sup> , Sihyung Lee <sup>4,‡</sup>  and Seung Yeob Nam <sup>2,\*,‡</sup> 

<sup>1</sup> Department of Computer Science, Federal Urdu University of Arts, Science & Technology, Islamabad 44000, Pakistan

<sup>2</sup> Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, Republic of Korea

<sup>3</sup> Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan

<sup>4</sup> School of Computer Science and Engineering, Kyungpook National University, Daegu 41566, Republic of Korea

\* Correspondence: synam@ynu.ac.kr

† These authors contributed equally in writing original draft preparation and review.

‡ These authors contributed equally in review and editing.

**Abstract:** Despite the rapid expansion in the insurance industry, many issues remain unresolved and may require immediate action. As the insurance sector continues to evolve with the development of new technologies, it faces more challenges, especially related to data security and fraud. The fraud-prevention data and tactics presently used by insurance firms are outdated and ineffective. Additionally, insurance firms have traditionally handled the settlement of all consumer claims through lengthy manual processes. These manual processes need to be changed to provide opportunities for insurance businesses to grow. In the case of vehicles, the information obtained from an automobile data recorder can be used as evidence. Data from automated vehicles are critical because they can help the police, law enforcement agencies, and insurance companies to reconstruct the events leading up to a collision. Insurance companies require the forensic analysis of accident videos, which is a time-consuming process and involves a large amount of storage. Due to hardware limitations and associated costs, the current standalone (and often dedicated) computing infrastructures used for this purpose are quite limited. Previous research focused on simple video analysis tasks within cloud computing and blockchain technology. The requirements for a large-scale auto-insurance system are quite high and need more thorough investigation. In this paper, a review of the contribution of recent approaches to storing accidental data in cloud computing using blockchain is provided. We focused on the latest cloud and blockchain studies related to auto-insurance along with the related issues and challenges. Some useful solutions and recommendations are provided to address the identified issues and challenges in the cloud-based and blockchain-based auto-insurance sector.



**Citation:** Mateen, A.; Khalid, A.; Lee, S.; Nam, S.Y. Challenges, Issues, and Recommendations for Blockchain- and Cloud-Based Automotive Insurance Systems. *Appl. Sci.* **2023**, *13*, 3561. <https://doi.org/10.3390/app13063561>

Academic Editor: Zheng Chang

Received: 10 February 2023

Revised: 5 March 2023

Accepted: 7 March 2023

Published: 10 March 2023



**Copyright:** © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

**Keywords:** blockchain; cloud computing; auto-insurance; insurance fraud; smart contracts

## 1. Introduction and Background

The insurance industry has grown rapidly in the last decade. Due to its rapid growth and the developing economy, it is a common target for fraud. According to Thomson Reuters [1], insurance fraud costs approximately USD 40 billion annually. Different types of vehicle insurance frauds (scams) have been uncovered by The Federal Bureau of Investigation in the United States, including staged accidents, false claims by policyholders, and falsified records for claims [2–6]. Various mechanisms and frameworks have been adopted to cope with these scams. In this regard, a number of tamper-proof models have been created to enhance the overall architectural security for better data management, improved communication within the network, greater credibility in data sharing among peers, and decentralized payment models for the automotive industry.

In the case of an incident, the insurance claimant has to proceed through various steps. In the past, insurance inspectors had to visit the event/accident site to obtain evidence. As a result, they had to spend a lot of time gathering and analyzing data before sharing their reports and supporting documentation with the relevant authorities. However, due to advances in technology, insurance policyholders have dashboard cameras that record incidents when they occur and send videos to insurers for immediate action. As these videos come in a variety of formats, some have copyright issues, which make storage and playback difficult. Moreover, there is the risk of information leakage during video transfer. These videos should be accessible to insurance inspectors and other authorized staff members for review and analysis. Insurance firms, however, find it difficult to save, retrieve, and analyze these videos. Due to the increased competition in the market, insurers are under pressure to process claims faster and maintain accuracy to avoid fraud. Therefore, insurance companies are turning to video-based forensics to overcome the serious challenges posed by modernizing corporate operations and reducing costs.

These challenges are faced by various organizations in addition to insurance companies. These organizations benefit from cloud computing. Cloud computing provides services over the Internet, including servers, data storage, databases, networking, software, analytics, and intelligence. This enables faster innovation, adaptable resources, and cost saving. Scaling up or down in the cloud allows for lower operational costs and better infrastructure management. To access the computing power, storage, and databases, one can use technological services from a cloud provider as needed, instead of purchasing, running, and maintaining physical data centers. Although cloud computing provides services using the Software as a Service, Platform as a Service, and Infrastructure as a Service models, cloud data security depends on third parties. Blockchain guarantees data protection and integrity without involving third parties. Companies are now exploring how to prevent fraud in various sectors using blockchain technology [7]. Blockchain [8–10] is similar to a linked-list data structure, where each block in a blockchain contains immutable data and is linked to its predecessor through a verified reference. Every block has a distinct header and body. The header contains the block version, previous block hash, time stamp, nonce, and Merkle tree root hash. The body portion contains the transaction counter and transactions. Each transaction contains an ID, sending address, fee, receiver address, and other pertinent data. Every blockchain node has access to all completed transactions. Blockchain is not easy to tamper with because each block contains a hash value of the previous blocks. Blockchain is more transparent than centralized third-party transactions, as transactions cannot be deleted once they have been added to the blockchain [11]. This infrastructure supports data security and prevents tampering attempts.

Rapid advances in technology are making it easier to store and process digital data in the form of text, audio, or video. These collective data affect every aspect of our lives. Due to the importance of these data, the aspects of security and authenticity require more attention. These digital data are stored on local systems or the cloud, which are vulnerable to attacks and can easily be tampered with. Various technologies and frameworks have been designed to enhance data security and authenticity. Blockchain is one of the leading technologies. Emerging technologies based on the cloud and blockchain have a significant impact on our daily life routines, especially in the auto-insurance sector. To assess the advantages and disadvantages of the technology itself, it is important to understand the problems and opportunities in the field. In this regard, different advanced cloud computing and blockchain auto-insurance models have been proposed. The purpose of this study was to review and survey the state-of-art existing cloud- and blockchain-based insurance systems. Several researchers and practitioners have published state-of-art analyses related to the different factors that have a direct impact on insurance stakeholders (policyholders and service providers), such as those found in [12–15], and blockchain- and cloud-based insurance frameworks and techniques have been discussed in [16–28].

The authors of [12] studied the different data-mining techniques used for fraud detection in auto- and medical insurance. In addition to fraud identification, knowledge related

to insurance is also important because customers often struggle to obtain enough benefits or receive inappropriate insurance due to a lack of literacy. From this perspective, Hongbing, in [13], provided an analysis of the existing research to develop consumers' insurance literacy. In this study, the author highlighted the connection between insurance education, literacy, and the behaviors of different stakeholders. These stakeholders' behavior and customer knowledge help the customers to make decisions regarding the continuity or discontinuity of the insurance policy. Wang, in [14], examined 60,000 vehicle insurance policies using machine learning techniques and determined the factors that had a direct impact on the clients' decision-making processes related to the continuity of the insurance. Regardless of insurance literacy, Arumugam and Bhargavi, in [15], drew attention to the driver's behavior. Driving behavior has a direct impact on the increase in traffic accidents. The survey in [15] explored many strategies to reduce the likelihood of traffic accidents, as well as the emotions, behavior, and activities of aggressive drivers.

In addition to the previously mentioned factors, the survey article by Gao et al. [16] emphasized the significance of telematics, which maintains data in the cloud and employs convolutional neural networks to classify drivers. Another review article [17] highlighted the vital role of cloud computing in terms of productivity, finance, business, on-demand infrastructure, and database applications. Although cloud computing has many significant impacts on different sectors, there are still security concerns regarding the use of cloud computing [18]. These security concerns can be tackled by implementing blockchain. Brophy [19] emphasized the use of blockchain for insurance-related transactions. The study presented in [20] identified subprocesses of insurance that could be enhanced using blockchain. In another systematic literature review [21], the authors investigated how the rapidly evolving blockchain technology will greatly impact multiple stakeholders in financial services. Chen et al. [22] investigated the challenges and gaps in blockchain-based smart contract applications. Although blockchain is a potential solution to cloud security challenges, blockchain also has security concerns, as highlighted by [23]. The combined use of blockchain and cloud computing can deal with many challenges; Xie et al. [25] focused on how blockchain can be used for cloud exchanges. Moreover, Artificial intelligence (AI) could play a significant role in the insurance sector. Eling et al. [26] proposed that AI could significantly improve and change the risky environment of the insurance industry. The research study presented in [27] demonstrated the widespread and successful use of data-mining- and artificial intelligence (AI)-based techniques for the detection of auto-insurance fraud. Gupta et al., in [28], used deep learning models to classify denial-of-service (DoS) attacks for security purposes.

The surveys presented in [12–28] highlighted various possible research directions that could help to enhance the insurance sector.

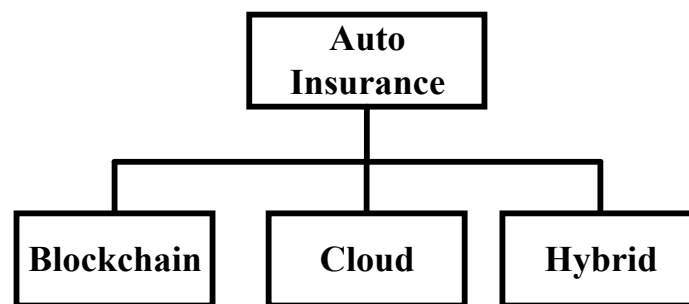
1. Unfortunately, insurance fraud, which has a detrimental effect on the functioning of the insurance sector and causes losses of millions of dollars every year, was not a research focus.
2. This state-of-art review article addressed cloud- or blockchain-based auto-insurance solutions. To the best of our knowledge, no review article has discussed the use of cloud- or blockchain-based auto-insurance systems to avoid fraud.
3. The authors of [12–28] discussed different problems according to the scope of each article. However, the issues and challenges related to existing blockchain and cloud computing insurance systems were not addressed.

This study's primary contributions are as follows:

1. Our survey investigates state-of-the-art auto-insurance solutions that are based on either the cloud or blockchain.
2. We explore and review the pertinent literature, highlighting important characteristics and challenges for currently available forms of cloud- and blockchain-based auto-insurance. In this way, our work offers a comprehensive analysis of the existing research. Based on this, we conducted a gap analysis that identified research gaps to provide academics and practitioners with potential research directions.

3. The survey exposes various issues related to auto-insurance and offers suggestions on how to address these, as well as suggesting areas for future research.

The rest of this paper is structured as follows. The literature review in Section 2 shows how our study differs from earlier reviews and surveys. Section 3 summarizes the research on cloud-based and blockchain-based auto-insurance, highlighting both the advantages and drawbacks. Section 4 lists the major issues and challenges in auto-insurance solutions. Section 5 presents suggestions for cloud- and blockchain-based vehicle insurance based on the major concerns and challenges that were identified. Section 6 offers future directions and recommendations for further learning and research into handling the identified challenges. Finally, Section 7 concludes the paper. The overall discussion presented in the paper is divided into three categories for convenience, as shown in Figure 1.



**Figure 1.** Categories of selected surveys and review papers.

## 2. Literature Review

Blockchain and cloud computing technologies appear to be successful in a variety of fields. In this section, we briefly present prior reviews and surveys related to auto-insurance, cloud computing, and blockchain technology, in addition to AI and ML techniques that have been applied in the insurance sector and some other fields.

### 2.1. Reviews and Surveys of Insurance Systems

The risks and challenges related to the insurance sector have been discussed in the literature, along with their solutions and frameworks. Many reviews and surveys have summarized these challenges while considering different factors. Sithic and Balasubramanian [12] summarized several approaches to financial fraud detection in the auto-insurance and medical domains. They studied the impact of different data-mining techniques on numerous types of fraud that can occur in these sectors. The main focus of their survey was to elaborate on fraud detection strategies based on data-mining techniques. They divided financial fraud into four categories: commodities fraud, securities fraud, insurance fraud, and bank fraud. One of the disadvantages of the study was the use of artificial data instead of real data.

The purpose of the study presented in [13] was to review and analyze the body of existing research in order to develop a more consistent measure of consumers' insurance literacy. It also highlighted key constraints in the insurance sector. A theoretical framework was developed that explained the connections between insurance literacy, insurance education, behavior, and well-being. This study provided a framework for ongoing research into customers' insurance literacy, which benefited both insurance and financial literacy.

The authors of [15] analyzed several factors, such as driving activities, habitual emotions, and aggressive driving behaviors, that result in traffic incidences. Their survey was designed to investigate various strategies to lower risks on the road by accounting for the emotional components that influence driving styles and behavior. They proposed that insurance companies use drivers' behaviors and emotional data from personal mobile devices to develop an ideal usage-based insurance premium package for risk prevention. It was also suggested that insurance companies can encourage safer driving by offering lower

premiums to certain clients. The main emphasis of the study was user-based insurance that considers how people perform and behave while driving.

Arumugam and Bhargavi, in [15], showed that insurance companies can propose policies according to people's behavior. However, they neglected the factors that affect policyholder decisions. In this regard, data from more than 60,000 auto-insurance policies were collected and examined by Wang [14], who implemented an ML algorithm to identify the main factors that influence consumers' decisions to continue using a particular insurer. The use of ML techniques by businesses to extract potentially useful information has become a hot topic in research on large insurance firms. The light gradient boosting machine algorithm, gradient boosting decision trees, and random forest were examined in this study and found to be the most effective models.

## 2.2. Reviews and Surveys of Cloud-Based and Blockchain-Based Insurance Systems

A survey on the topic of telematics, which deals with vehicle-driving data stored in the cloud, was presented by Gao et al. [16]. They discussed car-driving data, outlined the challenges associated with telematics data cleansing, and emphasized the problem of car-driving data openness in telematics. The authors of [16] studied different neural network techniques. The experimental results proved that the convolutional neural network could successfully classify various car drivers depending on their driving styles with high accuracy. They proposed two methods for increasing the accuracy of claim-frequency prediction using telematics data: one based on telematics heatmaps and the other on time series of individual trips.

Akhosama and Motoori examined insurance companies that employ cloud computing using a descriptive and analytical survey method [17]. Cloud computing was examined in terms of its productivity, business, on-demand infrastructure, finance, and database applications. A total of 33 insurance companies in Kenya were studied. Information from the respondents was gathered through observation and a standardized questionnaire. The survey suggested that insurance companies should make additional investments in infrastructure, capacity expansion, staff training, and cloud computing security.

Although there are many advantages of cloud computing, there are also some issues related to security. The study presented in [18] explored the security concerns that arise from the data lifecycle when a company uses cloud computing. A framework for data management was introduced in [18], which included data classification (business and personal) and risk management. The study claimed that administrators can identify the application and data and suggest appropriate security controls.

Security issues in cloud computing can be overcome using blockchain technology. The potential for blockchain integration in the insurance industry was explored by Brophy [19], who illustrated how transparency and regulatory compliance are facilitated through auditability. Endorsing the use of blockchain for efficient insurance-related transactions, the developer created an open-source permissioned blockchain platform called Hyperledger Fabric.

The study presented in [20] described how blockchain-based investments can benefit the insurance industry. This article covered the basics of blockchain and key platforms, providing a simple theoretical rationale for the insurance subprocesses that blockchain can improve. Some of the challenges that need to be overcome before blockchain technology is fully implemented in the insurance industry were also covered.

Although blockchain is a new technology, it has been used in many applications. Through a systematic analysis of the literature, the authors of [21] discussed blockchain's applications in the financial services sector. Research findings from many studies and publications revealed that blockchain may be useful to both academics and practitioners in the financial services industry. The study presented in [21] investigated how rapidly evolving blockchain technology could lead to a fundamental change in this sector, holding great potential for numerous stakeholders in the financial services business. Their analyses were limited to the adoption of blockchain for use in financial technology. Numerous other

blockchain applications, including Bitcoin, healthcare, advertising, insurance, energy, and societal uses, were discussed in [22]. This study provided a timely summary for people and businesses interested in adopting blockchain technology. It comprised an exhaustive study of real-world smart contract applications using blockchain and the associated challenges, emphasizing issues and knowledge gaps that need to be filled. The review focused on how blockchain technology is used in the healthcare industry to address scalability issues and deliver solutions. The survey was primarily designed to spur the development of more blockchain applications.

Li et al. [23] explored recent cyberattacks on the Ethereum, Bitcoin, and Monero systems. They discussed the security challenges faced by blockchain and solutions to hidden threats. Three types of assault, susceptible attacks, privacy leakage, and double spending, were mentioned in [23]. The authors suggested blockchain-based 6G network solutions, including support systems and cryptographic algorithms. They studied the strengths, weaknesses, opportunities, threats (SWOT) matrix to analyze the benefits, drawbacks, opportunities, and risks connected with the transition from a traditional account to a blockchain account. They highlighted the basic reasons for the serious vulnerabilities in smart contracts, although it should be noted that only the technical aspects were discussed. Although these strategies are beneficial, little attention has been paid to how developers actually work with the underlying programming languages, which could lead to the creation of defective codes [24].

In order to overcome the weakness of both cloud and blockchain technology, many sectors use a combination of these services in their applications. Xie et al. [25] focused on the use of blockchain technology in the cloud and the associated issues. They described how blockchain could be used for cloud exchange (CloudEX). Recently, the concept of CloudEX was introduced as a possible solution in the delivery of a single cloud service, where customers and suppliers are allowed to post their demands and offers. The study discussed the advantages of using blockchain to provide and manage connections between various cloud services. An overview of CloudEX was provided, and then blockchain technologies were discussed briefly before addressing the problems associated with blockchain in regard to privacy, security, transaction management, and reputation systems. Finally, the advantages of using blockchain to provide and manage the connections between various cloud services were highlighted.

### *2.3. Reviews and Surveys of AI- and ML-Based Insurance Systems*

In addition to studying and using blockchain and cloud computing, the insurance sector additionally employs AI and ML. Eling et al. in [26] and Benedek et al. in [27] provided overviews of big data applications for AI in the insurance sector and evaluated their impact. The authors of [26] provided some further insight based on their assessment of the current expectations, derived from these results, for different potential solutions. The study demonstrated how the insurance industry's business model is changing from one that prioritizes loss compensation to one that focuses on cost efficiency and new revenue sources. The authors suggested that AI may significantly alter the risk environment for the insurance sector. For this reason, insurance companies must reconsider their conventional insurance coverages and produce appropriate insurance solutions accordingly. The study presented in [27] focused on the significance of AI and data-mining techniques for identifying auto-insurance fraud and highlighted the associated problems caused by data instability, as well as the lack of cost-sensitive techniques.

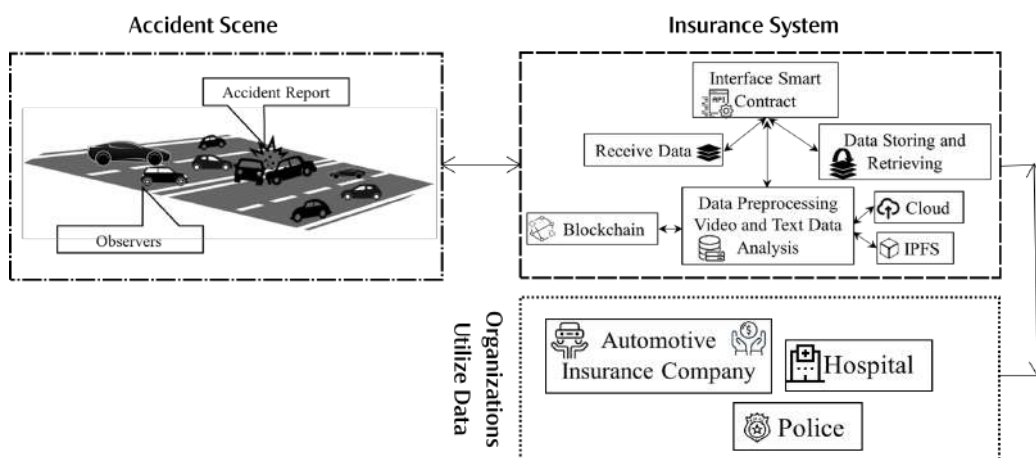
In order to implement AI in the vehicular sector, vehicles are being automated. This automation increases risk from a security perspective. Gupta et al. [28] investigated the classification of threats from autonomous vehicles by utilizing service availability, accountability, and authentication. The deep learning techniques long short-term memory and deep neural networks were presented in [28] and used to identify DoS attacks. The paper conducted a comparative analysis of their use against the backdrop of significant 4G and 5G deployments. A critical merit of this study was that it included a taxonomy of au-

tonomous vehicle attacks. However, in this survey article, safety concerns and applications for vehicles were not considered.

The goal of these reviews and surveys was to examine several key blockchain and cloud computing concepts, technologies, and application areas; however, they did not provide an in-depth analysis of the techniques, current issues, and advancements in cloud- and blockchain-based auto-insurance. Compared to our work, most of the previous surveys addressed only one, or a few, of the security and privacy problems, without addressing security remedies. Therefore, previous surveys were typically more narrowly focused on a specific challenge or technical issue. To the best of our knowledge, our article is the first work to provide a brief survey of the current challenges and solutions for cloud- and blockchain-based auto-insurance.

### 3. Auto-Insurance Systems Based on Cloud or Blockchain

In this section, we present previous studies from the pertinent literature that investigated the problems and challenges related to cloud computing and blockchain in the auto-insurance industry and proposed solutions accordingly. Auto-insurance systems are being automated to avoid fraud and delays in insurance claims. In this regard, some insurance companies are storing data (videos related to accidents and information about policyholders) on the cloud and conducting insurance transactions through the blockchain network, as shown in Figure 2. The insurance system in Figure 2 can collect traffic-event-relevant data from the vehicles, user devices, etc.; store or retrieve the data on various types of storage systems, including IPFS and cloud; analyze the video data; and provide the data or analysis results to other organizations when they are requested. Each block in the insurance system can be implemented as an application running on a node with computing capabilities or as a smart contract in the blockchain.



**Figure 2.** Systematic graphical representation of a cloud- and blockchain-based auto-insurance model.

In an effort to create fundamental video analytic functions, some recent research efforts have collected accident videos from dashboard cameras and stored them on blockchain and the Interplanetary File System (IPFS). The main goal of this section is to introduce the reader to the numerous image and video storage techniques for the insurance sector based on blockchain, cloud computing, and hybrid systems.

#### 3.1. Blockchain-Based Auto-Insurance Applications and Frameworks

By establishing coverage between policyholders and insurance companies, blockchain can automate claims processes and the settlement of claims between parties, reducing the administrative costs incurred by insurance companies. Additionally, insurance companies can use a blockchain to store and retrieve accident videos that are captured from vehicles and their surroundings. In this subsection, we present the current blockchain-based techniques and approaches in the auto-insurance sector. In this section, we discuss

articles [29–36] and identify various mechanisms, such as data tampering, multiple insurance, and transaction-related challenges and their solutions. However, each article highlights a specific problem with the solution. We identified the advantages and issues in the aforementioned blockchain-based auto-insurance solutions and summarized them in Table 1.

A lot of research has been conducted on blockchain and applied to many fields in recent years. However, blockchain technology has not yet been fully explored in the insurance industry [29]. Gattischi et al. [29] discussed insurance businesses that use smart contracts, emphasizing the strengths, shortcomings, opportunities, and risks of blockchain technology. This study investigated use cases based on smart contracts in the insurance sector domain and left the readers to make the final decision regarding the actual benefits that can result from the use of this technology in a particular context. Demir et al. [30] presented a blockchain-based car insurance administration system that addressed issues of collaboration, security, data privacy, transaction costs, scalability, and availability. According to the authors, blockchain could be used to create an insurance record system that can handle all aspects of insurance transactions. This blockchain-based system includes drivers, dealers, insurance firms, lawyers, and law enforcement agencies. In this regard, ref. [31] implemented a blockchain-based pay-as-you-go car insurance application to ensure transparency. This application ensured that all data related to the user's actual journey were recorded transparently. The research was initially undertaken by IBM Research in Australia, and all parties involved in the insurance contract were confident that the data were tamper-proof and traceable.

In the insurance sector, fraud is a major problem that costs a lot of money [32]. Roris and Pereira [32] proposed a blockchain-based solution to prevent fraud in automobile insurance. It was demonstrated that blockchain technology could be used to identify vehicle insurance fraud and reduce insurance company losses. The main objective of the work presented in [32] was to deal with double dipping, which is defined as follows: "exploiting multiple insurance policies of the same vehicle in different companies". To overcome the problem of double dipping, smart contracts were designed to validate claims and record the lifecycle of a vehicle in the blockchain. Data tampering is another type of fraud. A blockchain-based framework for auto-insurance claims and adjudication (B-FICA) was proposed in [33], a framework based on tamper-proof documents and immutable blockchain transactions.

Oham et al. [33] provided a complete framework for vehicular network forensics using blockchain technology. The authors used a permissioned blockchain and online tracking technique in which data were instantly provided to the registration authority or witnesses who were present during the data exchange. Using a permissioned blockchain, the system protected users' privacy by limiting the transactions that participating companies were authorized to make or view. This privacy-friendly liability model provided untampered proof for liability attribution and adjudication in the event of an accident. It used anonymous certificates to provide pseudonymity for a specified period of time. The ubiquitous set of connected automated vehicles (CAVs) used automotive sensors and communications to collect data to establish indisputable claims and send them to third parties. Direct communication without the involvement of a third party is always considered more secure. A mobile application called Dia-LOG presented in [34] enables communication between vehicles and authorized devices to collect transactions, and provides integrity and data protection to support digital forensic investigations. Dia-LOG is a reliable and secure privacy protection mechanism that effectively creates an automotive logging system specifically for forensic data collection and storage. Endpoint detection and response (EDR) is recommended as a way to capture data after authentication using a personal mobile device while accessing recorded data. Despite this solution, it is clear that analyzing raw controller area network (CAN) messages requires the reverse engineering of message syntax and semantics, the reconstruction of vehicle dynamics, and the decontextualization of messages and their content. This requires the manual inspection of large amounts of data. In the event of an



accident, EDR stores vehicle data for investigation purposes. Investigators also use forensic data loggers that continuously store vehicle data, such as speed and accelerometer readings.

Another traffic accident investigation system was proposed in [35], which used the digital data generated by numerous sensors in a vehicle. The authors adopted blockchain-based technology to investigate traffic incidents in self-driving vehicles. They mentioned that it is difficult to evaluate the data in terms of video analysis, because drivers may damage the video, the recording may not be complete, or the driver may refuse to collect it. The use of the unique information provided by sensors, as well as digital forensics analyses with data integrity, could help to overcome the analytical challenges created by poor video quality. A witness-based data priority mechanism (WIDE) was introduced by Oham et al. [36] for vehicles in the vicinity of an accident. As soon as an accident occurs, WIDE assesses the integrity of the data produced by vehicles (referred to as witnesses) to ensure the trustworthiness of the information that will be utilized to determine the liability of each driver. In the WIDE model, a two-level integrity assessment is used, which first verifies the reliability of the sensors that provide the data before ensuring that the data are not changed during transit. It also prioritizes witness data and ensures that only the most reliable witness information is used.

A blockchain-based architecture for the vehicle insurance sector was presented in [37], which manages and automates the claims payment process. The proposed car insurance policy model (CAIPY) was an ecosystem for vehicle insurance. This model was based on the IPFS and blockchain-based infrastructure of the vehicle insurance sector, which makes insurance claims transparent and tamper-proof using Ethereum smart contracts. Smart contracts can assist parties in establishing the required trust by safeguarding the contract inside a blockchain [38]. The physical insurance policies between consumers and insurers served as a model for the pieces used in the creation of CAIPY. To store vehicle health information, smart contracts are installed separately and communicate with sensors.

In addition to auto-insurance, many blockchain models have been proposed to deal with insurance fraud in the health sector. A blockchain-based application [39] was developed to improve current health insurance business practices. The technique aimed to detect fraud in health insurance using data collected from all insurance firms [40]. Amazon Web Services (AWS) and BigchainDB were used to create a blockchain system wherein MongoDB stored the blocks in each node of BigchainDB. The proposed system was evaluated with unit testing, integration testing, system testing, smoke and regression tests, and performance testing.

**Table 1.** Advantages and limitations of existing blockchain-based insurance models.

Ref.	Advantages	Issues/Limitations
[29]	A shared ledger technique is presented, which has low risk and great reliability and can assist insurance firms and third parties in calculating premiums.	The authors of the SWOT analysis summarized the benefits and drawbacks of blockchain technology. The SWOT analysis produced a one-dimensional model, in which each problem attribute was classified as a strength, weakness, opportunity, or threat. Each attribute had only one effect on the problem under consideration, although, in actuality, it may have both strengths and weaknesses.

Table 1. Cont.

Ref.	Advantages	Issues/Limitations
[30]	<p>i. A blockchain technique based on Hyperledger Fabric was used to collect insurance data, and all the transactions and related smart contracts were validated.</p> <p>ii. The suggested approach used public keys to keep users' identities safe.</p>	<p>i. IoT data volumes and timely communications were major challenges for the proposed system.</p> <p>ii. There was no discussion about the implementation or about the results achieved by the proposed system.</p>
[31]	<p>Pay-as-you-go auto-insurance was offered, whereby drivers are charged based on the distance they travel and are protected against newly emerging hazards such as cyberattacks.</p>	<p>There were suggestions regarding the handling of some off-chain transactions through the adoption of permissioned ledgers. This type of ledger has a control group of users but no incentives; therefore, mining incentives would have to be determined.</p>
[39]	<p>i. A blockchain-based approach was proposed to detect health insurance fraud that utilized the data acquired by all insurance companies.</p> <p>ii. The suggested approach improved current business processes for health insurance.</p>	<p>i. Certain users could change blocks, which goes against the core BC fundamentals.</p> <p>ii. Furthermore, the authors did not evaluate the proposed system.</p>
[40]	<p>The proposed system was discussed, along with its design artifacts and implementation.</p>	<p>This work was too complex, owing to the use of many different tools.</p>
[32]	<p>i. The authors demonstrated how blockchain may be used to construct a vehicle insurance system that prevents certain sorts of fraud.</p>	<p>i. This study was a preliminary study based on a prototype.</p>
[33]	<p>i. To create unquestionable assertions and convey them to external parties, this study made heavy use of CAVs to gather data from automobile sensors and communications.</p> <p>ii. Due to its immutable blockchain transactions and tamper-proof records, B-FICA was shown to be secure. It provided temporary anonymity certificates.</p>	<p>i. To establish data consistency, the authors relied on data from witnesses; however, they did not evaluate the authenticity of the data obtained from the witnesses, or the possibility of the exploitation of data created by a vehicle after being forwarded as evidence.</p>
[34]	<p>i. A robust and secure privacy-preserving mechanism was introduced to construct a vehicle-logging system to store forensics data.</p> <p>ii. The experiments could help other researchers to better comprehend the semantics of CAN signals.</p>	<p>i. Such approaches frequently necessitate the reverse engineering of CAN communications.</p> <p>ii. The main issue with this research was that the vehicle's driver knows and decides which data will be stored.</p>

Table 1. Cont.

Ref.	Advantages	Issues/Limitations
[36]	Data integrity was guaranteed with a two-level integrity evaluation approach.	<ul style="list-style-type: none"> <li>i. WIDE did not consider privacy issues, with witness vehicles supplying information to expedite responsibility judgments.</li> <li>ii. The proposed work did not consider issues such as scalability, execution times, and storage limitations.</li> </ul>
[35]	<ul style="list-style-type: none"> <li>i. The authors provided information on numerous functional facets of the vehicle ecosystem that could benefit from blockchain technology.</li> <li>ii. As every transaction was tracked and tamper-proof, the proposed framework proved to be successful in automatically handling insurance claims and resolving conflicts among different stakeholders.</li> </ul>	No proper mechanism was defined to deal with double dipping, which must not be ignored [33].
[38]	CAIPY could be expanded to include more robust access control. Smart contracts were utilized to determine insurance premiums, and blockchain was used to store encrypted driving data.	Symmetric encryption keys were used, but a major problem was the need to disclose the key to the person with whom the data were exchanged. Since just one key was used for symmetrical encryption, it was known by both the sender and receiver.

### 3.2. Cloud-Based Auto-Insurance

Cloud computing has the potential to benefit insurance companies in a number of different areas. The cloud makes it possible to access new promotional strategies and methods, as well as to boost customer loyalty and retention. In this subsection, we discuss the recent attempts to store data consisting of videos or images of accidents taken from dashboard cameras to perform video analytic operations for insurance and other purposes. The benefits and issues of the related cloud-based vehicle insurance frameworks [41–48] are listed in Table 2, and their working infrastructure is discussed below.

Table 2. Advantages and limitations of existing cloud-based auto-insurance models.

Ref.	Advantages	Issues/Limitations
[41]	<ul style="list-style-type: none"> <li>i. A cloud-hosted, dynamic, front-end visualization was presented to assist relevant authorities in conducting holistic data analyses.</li> <li>ii. Through an evaluation of the stored and processed data, companies could make decisions.</li> </ul>	<ul style="list-style-type: none"> <li>i. A stored accident video was accessible without authorization.</li> <li>ii. The message-passing mechanism was not elaborated in detail.</li> </ul> <p>The suggested program was complex due to the involvement of many sensors and technologies, such as edge and cloud computing.</p>
[42]	An app allowed for users to record real-time videos using AES-128 encryption and save them to the cloud for backup.	<ul style="list-style-type: none"> <li>i. The application was limited to Android-based mobile devices.</li> <li>ii. Drivers record live video, encrypt evidence, and save it to the cloud.</li> </ul>

Table 2. Cont.

Ref.	Advantages	Issues/Limitations
[45]	<ul style="list-style-type: none"> <li>i. The project focused on the application of cloud computing in accident response systems, such as hospitals and drivers.</li> <li>ii. The web browser could provide a variety of services that are necessary in vehicles, hospitals, and on the roadside.</li> </ul>	<ul style="list-style-type: none"> <li>i. Smart gadgets and sensors must be installed inside every on-road vehicle for real-time protection.</li> <li>ii. It was difficult to gather original data.</li> </ul>
[46]	<ul style="list-style-type: none"> <li>i. MATCH provided a straightforward technique for using a smartphone to take images of a damaged car and transmit the initial notification report to the insurance company.</li> <li>ii. Additionally, a map with the phone numbers of neighboring medical facilities and towing companies was shown.</li> </ul>	<ul style="list-style-type: none"> <li>i. During serious accidents, mobile phones might break, or their batteries can die.</li> <li>ii. An accident could occur in a location with poor, or no, mobile signal.</li> </ul>
[47]	The car instantly uploads its auto-insurance history to the cloud. More importantly, a car involved in an incident must immediately provide the insurance provider with the necessary paperwork and vehicle information, so that it may be processed.	<ul style="list-style-type: none"> <li>i. The development of the centralized parking system was not covered in this study.</li> <li>ii. There was little discussion of the auto-insurance process.</li> </ul>
[48]	<ul style="list-style-type: none"> <li>i. AES is a faster and more secure algorithm because it has a comparatively large secret key.</li> <li>ii. AES is open-source and resistant to hacking attempts due to its longer key size (128, 192, and 256 bits).</li> </ul>	<ul style="list-style-type: none"> <li>i. The algebraic structure used in the proposed work was extremely simplistic, and each block was encrypted with the same pattern.</li> <li>ii. The software implementation of AES in counter mode was difficult, especially when performance and security are considered.</li> <li>iii. The randomization efficiency of the proposed system was about 70%.</li> </ul>

In [41], accident alerts from all vehicles equipped with OBUs were collected and sent to the nearest hospital using an open-source web server program. Following the rescue procedure, the collected data were transmitted to edge and cloud storage. The stored data could be retrieved and thoroughly evaluated by the police, courts, and insurance companies. In addition to data transfer, data reliability is also important for the prevention of data tempering or loss. A mobile application for Android phones was designed to store real-time video and a Google Maps journey as evidence [42]. The data were protected against loss and tampering by unauthorized users in the cloud using the advanced encryption standard (AES)-128 encryption method. Car owners, insurance companies, and other investigation agencies could benefit from this application. Authorized individuals could view the recorded data, whereas encryption prevented unauthorized individuals from editing or manipulating these data. Similarly, using cloud computing techniques, the research presented in [45] provided solutions for life-critical systems following an accident. Sensors in an automobile system were employed to increase safety and relax the driver. Another mobile application called MATCH [46] offered a simple method for taking pictures of a damaged car and sending an initial notification to the insurance company from a smartphone. Additionally, a map with contact information for neighboring hospitals was displayed. The authors claimed that this application would be quite helpful in reducing human labor by allowing people to file insurance claims with just one click.

In addition to accidental information storage, Magsino [47] proposed a centralized cloud-based smart parking system in addition to the storage of accident information for insurance reports. If necessary, real-time reporting can be used when autonomous vehicles require repair work or assistance. Using either roadside infrastructure or a cellular network, an intelligent vehicle can establish a connection to the cloud. Essentially, a vehicle involved in a collision must send the necessary paperwork and vehicle information to the insurance provider right away, and only once, for processing. The car immediately uploads its auto-insurance history to the cloud. More importantly, a vehicle involved in a collision must immediately provide the insurance company with the required documentation and vehicle details for processing. Cloud-based infrastructure has security threats that cannot be ignored. To ensure data security, a vehicle information management system [48] stores data in an encrypted form in the cloud. The client component provides a variety of forms and reports to present various plans and satisfy the needs of vehicle insurance management. The data are encrypted with an AES algorithm so that no one else can read them.

### 3.3. Hybrid Auto-Insurance

As discussed in the previous sections, cloud- and blockchain-based solutions have been proposed for the insurance sector to solve the problems of the existing manual systems. However, blockchain and cloud computing have their own advantages and disadvantages; thus, when combined, they could overcome each other's shortcomings and provide a better solution. A blockchain-based solution for vehicular forensics was introduced in [49], which integrated the involved entities and facilitated the provision of the data needed to settle disputes. This framework was used to collect vehicle data from drivers, maintenance centers, manufacturers, and other agencies and then upload them onto the cloud. Blockchain was adopted to monitor vehicle-related data, including maintenance information and vehicle diagnostics reports. The authors utilized driving data from the on-board diagnostics (OBD) port and EDR to provide valuable complementary evidence to resolve traffic accidents and disputes among parties. The solution proposed in [49] stored data in the cloud without considering data privacy. In this regard, the authors of [50] investigated and examined the numerous elements needed to protect privacy, as well as the privacy problems faced by CAVs. Singh et al. [50] proposed a hybrid cloud- and blockchain-based model in which the cloud was used to store data and the blockchain helped to secure data exchange due to its reliability and trustworthiness. In this approach, a consensus algorithm called proof of driving was used to authenticate the car within the network. The framework improved the privacy and secrecy of communication between vehicles by offering a rapid and safe infrastructure. All authenticated transactions were summarized in a Merkle tree, which was produced by repeatedly hashing the data and producing new Merkle roots. For each specified time slot, a hash value was assigned to each string collected in a local database. The Merkle tree was updated, and this hash value was added as a leaf node, resulting in the creation of a new block in the blockchain. This approach led to an intelligent data transmission system based on blockchain technology, smart connected vehicles, and vehicular cloud computing. Although vehicle automation helps in many ways, such as by establishing a faster and more accurate means of information storage and transmission, the dissemination of fake information cannot be ignored.

The issue of security problems in smart cars was examined by Oham et al. [51]. A permissioned blockchain-based reputation system was employed to prevent the dissemination of false information throughout the network. The authors introduced the B-FERL protocol, which monitored each vehicle's internal state and looked for instances of vehicle compromise. This system used a challenge–response data-exchange mechanism between RSUs and vehicles to keep track of the vehicles' internal health and spot any malicious activity in the network. Furthermore, only the previous and current transactions of each vehicle were stored in the network node to ensure scalability and forward other transactions to the cloud so that the previous record could be accessed when required. Health insurance is also an emerging field. A basic design for a cloud- and blockchain-based health insurance

system was proposed in [52] using sequence diagrams, a data management framework, a smart notification system, and a smart claims processing system. This work suggested a blockchain-based alternative to improve the National Health Insurance System (NHIS) in terms of financial sustainability in Ghana. The authors emphasized the significance of information quality, service quality, and user satisfaction as essential components in the adoption of an effective cloud- and blockchain-based solution. In this research, the authors discovered a significant relationship between user satisfaction and information quality. The benefits and issues in the aforementioned hybrid (i.e., cloud- and blockchain-based) vehicle insurance options are listed in Table 3.

**Table 3.** Advantages and limitations of hybrid (cloud- and blockchain-based) auto-insurance solutions.

Ref	Advantages	Issues/Limitations
[49]	A lightweight object application blockchain framework was proposed, which integrated DF processes and data privacy to provide efficient vehicle-related digital investigations. The stored data were only disclosed to an authorized party.	Block4forensic (B4F) was proposed with 100% support by a VANET blockchain; however, practically speaking, this is not realistic. Therefore, it is necessary to find out how much a blockchain system's performance is affected by the nodes' mobility in a VANET. B4F employed blockchain to achieve data integrity; therefore, it was prone to selective data sharing and data alterations, because the vehicle was in charge of determining which data were used as evidence to determine liability, and the integrity of the sensors that contributed the data was not considered.
[50]	The suggested system used crypto IV-TP and was based on rewards that provided records in case of accidents. The data were validated and audited using a smart contract. Vehicles were linked to the blockchain and had a special crypto number. Consistency in BC was guaranteed through distributed consensus mechanisms.	The strategy was not ideal for large datasets, such as multimedia data, because it would raise the cost of the vehicle's calculations and storage, which would eventually decrease system performance [53]. A malicious vehicle may purposefully transmit misleading information and confuse other vehicles to exploit the vulnerabilities of VANETs.
[51]	A permissioned BC-based reputation structure was introduced to prevent the spread of misleading information across the network. The records of automobiles were only handled by trusted parties.	The system was complicated as a result of the hybrid cloud environment, which consisted of both internal and external clouds.
[52]	Designing and implementing a blockchain-based solution to prevent the NHIS from going bankrupt was the goal of this effort.	The authors claimed that "the system achieves its objectives because all the write, delete, and modification operations were successfully executed in the worldstate and blockchain systems", but this was unclear, because blockchain does not permit alterations or deletions.

Thus far, we have identified and mentioned the primary issues (and challenges) related to blockchain- and cloud-based auto-insurance. The relevant studies are compared in Table 4 on the basis of the aforementioned issues and challenges.

**Table 4.** Research studies and their handling of current challenges.

Ref	Type	Security	Privacy	Access Control	Storage
[29]		✓		✓	✓
[30]			✓		
[31]			✓		
[49]	B	✓	✓	✓	✓
[39]	L		✓	✓	
[40]	O	✓	✓	✓	
[32]	C			✓	
[33]	K	✓			
[34]	C	✓	✓		
[37]	H			✓	✓
[38]	A	✓	✓		
[36]	I	✓	✓		
[45]	N				✓
[41]				✓	✓
[42]	C		✓	✓	✓
[46]	L		✓		
[47]	O			✓	✓
[48]	U		✓	✓	✓
[49]	D	✓		✓	✓
[50]			✓		✓
[51]	H		✓	✓	
[52]	Y	✓	✓	✓	✓
	B				
	R				
	I				
	D				

Table 4 demonstrates that storage (rather than security) is the primary focus of most research on cloud-based auto-insurance. Many insurance organizations consider using the cloud for storage to be fairly easy, because they do not have to worry about managing and expanding their storage. Additionally, cloud platforms have eliminated the requirement for local devices and many other services. Many organizations entirely rely on cloud service providers to keep their data secure and accessible. However, cloud infrastructures still face several internal and external threats to data integrity, and even well-known cloud providers suffer from outages and data loss [54]. In order to maintain their clients' faith and confidence, cloud service providers generally hide the issues with their cloud storage servers. Integrity issues in cloud computing can occasionally be caused by architectural problems [55]. However, the inability to ensure data confidentiality, integrity, and availability may limit the cloud's use by insurance companies. Table 3 demonstrates that the primary areas of most investigations related to blockchain-based vehicle insurance are access control, security, and privacy. Blockchain is more secure than cloud storage, but it has limited capacity. Decentralized blockchain storage takes advantage of the unused hard disk space derived from their users, which can also address several issues present

in a centralized system and is an alternative to centralized cloud storage. It would be helpful to take advantage of both systems (that is, blockchain and cloud computing). For example, it is difficult to store all video records in blockchain nodes, since they have a limited storage space compared to the cloud. Therefore, one option is to keep links to the original videos (along with other accident data) in blockchain nodes and to store the original videos themselves in the cloud (for example, on an IPFS or on YouTube with appropriate access privileges). In this way, auto-insurance companies can benefit from both cloud computing and blockchain technology (for example, gaining both immutability and sufficient storage space).

#### 4. Challenges for Insurance Systems

Auto-insurance is an emerging sector that generates a huge amount of annual revenue. According to the statistics, the worldwide cloud computing market is expected to reach USD 250.05 billion in 2021 and USD 791.48 billion by the end of 2028 [56]. Although cloud computing and blockchain have provided excellent support for the management of many diverse and complex problems, both technologies still face many hurdles and challenges. The main challenges are related to security, data privacy, resource access control, data storage, energy consumption, etc. In this section, we will discuss these challenges in more detail.

##### 4.1. Security

Security refers to protection against anything that can harm the system. In the cloud and blockchain contexts, various types of malicious attacks are possible. The security of insurance data needs to be further enhanced and standardized as some of the nodes can be compromised, which can interfere with the data [57]. Therefore, it is necessary to employ security in both blockchain and cloud computing to prevent the unauthorized access to and disclosure, copying, or editing of insurance data. The security and privacy of consumers' records is crucial in auto-insurance and requires a number of standards to be maintained. Some of the most common security and privacy concerns for vehicle insurance and the relevant data are presented below.

##### 4.1.1. Confidentiality

Confidentiality ensures that no unauthorized party has access to insurance-related information. One of the most important concerns with cloud computing and blockchain is data confidentiality, which ensures that data are only available to authorized users on the network. As a result, the service provider must ensure that unauthorized users do not have access to customer data. When a data owner shares confidential information with others via blockchain or the cloud, he or she usually loses control over those data due to the lack of physical control. In cloud computing, multiple jobs run at the same time, and clients use shared resources. As a result, there are concerns regarding confidentiality and the possibility of data leakage. Attackers might use methods such as packet spying, password attacks, port scanning, wiretapping, keylogging, and social engineering to compromise cloud confidentiality. Blockchain can ensure confidentiality at a particular stage. The data elements are transparent to every person who shares them with others in a single blockchain because of the blockchain's decentralized nature [58]. As a result, it is challenging to enforce confidentiality using blockchain. The decentralized nature of blockchain has major implications; for example, it becomes possible for anybody to view the transactions. Therefore, organizations maintain confidentiality and integrity in blockchains with the help of cryptography. Blockchain technology employs cryptography to sign communications and encrypt data using a private/public key scheme. Scams and illegal transactions can be identified using blockchain data. As a result, blockchain can effectively protect pseudonymity while also providing some level of confidentiality.



#### 4.1.2. Integrity and Immutability

The process of conserving data and ensuring consistency is referred to as data integrity. By informing customers about the status of their stored data, the service provider must ensure data integrity. A Sybil attack can be initiated to threaten the integrity of the cloud, in which an attacker creates a large enough number of bogus identities to influence the actual system and take control of the network. This can be conducted by either introducing new devices or subverting existing ones. An integrity management service is used by cloud providers to ensure data integrity through a third party. However, a fundamental weakness of this approach is the data owner's willingness to submit data integrity verification to a third party. Cloud computing must ensure reliability and prompt access for platform users, in addition to providing the usual services. If there is a problem on the server, the applications will not run, and data will not be available. Due to the increasing frequency of network failure in recent years, people have been worried about the reliability of cloud computing [59].

In a blockchain, the integrity of the saved data can be preserved due to the reliability of the P2P network, its well-formed transactions, and its authentication and auditing features. A Merkle-tree-based data integrity verification mechanism is also used in blockchain. If an attacker tries to change the data stored in the blockchain, he or she must first change the metadata. All peers maintain the same data based on the addition of new blocks to the blockchain, making the network impervious to subversion attempts. Moreover, a transaction that was registered in the blockchain cannot be removed or modified. The immutability of data is one of the most essential blockchain features, which improves its robustness, accuracy, and reliability. Immutability is accomplished with blockchain because data cannot be changed without the consent of the entire network. Usually, smart contracts are employed in blockchain to implement integrity, in which data are first locally encrypted and then synchronized with the data in all nodes throughout the entire network. The dependability of the records may be jeopardized if an open-source blockchain software contains bugs or weaknesses. The source code of many blockchains has significant bugs, which might cause an unintentional hard fork if exploited [60]. However, because a blockchain is distributed and decentralized, it is safer than the cloud. Since there is no single point of failure in a blockchain, fraud is much more difficult than it is in cloud computing. However, there is a trade-off between immutability and performance when using blockchain. In summary, many different factors contribute to the loss of integrity in insurance data (whether in a blockchain or in the cloud): (1) the number of devices; (2) the number of participants (data owners, insurance firms, security agencies, cloud service providers); and (3) the dynamic data sources.

#### 4.1.3. Availability

The term availability means that data are available when needed. Data availability is critical for a range of stakeholders, including insurance firms, data owners, and law enforcement organizations. However, unscrupulous actors may misuse the same data to generate major social and ethical problems. The more prevalent forms of cyberattack for insurers include DoS, data exfiltration, malware infections, financial transaction theft, zero-day exploits, and phishing emails [61]. The main effects of these cyberattacks on insurers include huge or significant expenses for customers and the company, as well as business interruptions. Distributed DoS is one of the most popular methods used by attackers to reduce system availability. The basic purpose of this attack is to bring a system down. Furthermore, availability attacks are commonly used as a prelude to spoofing or authentication threats. Another form of attack in the auto-insurance industry is to disable or restrict physical access to devices that are already dispersed across the network. In blockchain networks, the availability issues increase with the volume of transactions.

#### 4.2. Privacy

According to the general data protection regulation (GDPR), data privacy refers to the degree of control that individuals have over who has access to their personal data. Privacy is a serious issue for many organizations and applications [62]. Insurance companies and clients are both very concerned with data privacy. In the insurance industry, there are no clear norms for data ownership. Although a driver's record may be her or his property alone, an insurance inspector or police officer may also request access to those data. The privacy challenge motivates insurance companies to create rules and standards that clearly identify ownership boundaries. There should be a means to identify and minimize negative privacy implications, and decision-makers should be informed of these so that they can take appropriate measures. Privacy is a critical concern for cloud computing in terms of both legal compliance and user confidence and must be prioritized. Keeping vehicle records safe from each other, other insurance companies, and cloud service providers is a challenging task. In order to protect their own data, all insurance companies require specific access to records.

Due to legal and insurance issues, a vehicle's identity is usually tied to its owner. As a result, tracking a car may intrude on the privacy of its owner on a regular basis. The accident data used by insurance companies are based on vehicles that are in motion in several places and therefore pose serious and unique privacy concerns. When insurance companies conduct a video analysis for forensics investigations, the investigators may face privacy concerns. The video footage should be analyzed without breaching the privacy of the customer or organization. In a blockchain, data can be accessed with or without permission. In a private blockchain, a legal authority normally ensures the security, validity, and integrity of the blockchain. The majority of independent peers defend the blockchain's security and integrity within a public blockchain. The chain ledger in blockchain stores sensitive data in the form of transactions, which can be shared with and examined by authorized users. Although transactions can be made anonymously in blockchain, traceable clues can disclose identities and other associated information [63,64]. Transactions can be linked to IP addresses to reveal even more information about a user, and third-party programs that track users' various accounts (as well as their data) can be hacked and subverted. The real-time transfer of enormous amounts of information is essential to a blockchain network and its applications. Therefore, the next most important issue in blockchain technology is how to preserve user anonymity even when a malicious party has access to all transaction data inside the blockchain [65]. Another major concern with blockchains is transaction leakage, because block data are exposed to everyone on the network. Securing the driver's privacy is a key issue in the exploitation of vehicle and driving data in the auto-insurance sector.

#### 4.3. Access Control

Access control is a security technique that restricts who has access to certain resources in a computing environment. It is a fundamental security rule that lowers organizational risk and regulates access to resources after issuing a user's credentials and authorization. It prevents unwanted users from gaining access to the system. There are many access control issues in auto-insurance-related data owing to the diverse and increasing number of distributed devices. Therefore, identification is always necessary before accessing any system, service, or device. With the emergence of cloud computing, data access is becoming increasingly critical, because the provision of secure network file storage and access control is a challenging task for cloud-based auto-insurance [66–68]. There is no perfect access control model among the currently available security models [69]. In cloud computing, the difficulties regarding access control are associated with availability and confidentiality. When a valid user is refused access, there is a loss in availability, and unauthorized access results in a loss in confidentiality. Furthermore, an unauthorized user who reaches the control network can learn the communication protocol, launch different attacks [69], and make changes to the data that compromise data integrity. Therefore, access control is the

most significant challenge, because it has a direct impact on all security principles, such as privacy, confidentiality, integrity, and availability.

#### 4.4. Storage

The digital recording of data, files, and documents for future use can be defined as storage. A storage system can protect data using electromagnetic, optical, or other media and restore the data if necessary. Cloud storage [70] provides easy, affordable, and very reliable storage. Using cloud computing, insurance businesses and insurers can quickly access data, and they can use the data and patterns to develop new solutions that meet the needs of their customers [45]. Although cloud storage provides many advantages, insurance companies face other challenges, such as a lack of control, internet dependency, and even difficulties in migration. Blockchain technology offers immutable storage by only allowing for transactions to be added, never modified or withdrawn. Large amounts of data cannot be stored efficiently in a blockchain due to the replication across all nodes. Furthermore, as more data are processed, transferred, and stored, the computational complexity of running blockchain nodes increases, i.e., data storage in blockchain has a cost model that is different from traditional data storage.

#### 4.5. Other Challenges

In the next sections, we discuss the additional challenges that the auto-insurance industry can face with the use of the cloud or blockchain networks.

##### 4.5.1. Energy Consumption

A significant amount of energy is needed to provide consistent power for the hundreds of servers in data centers. Additionally, sending data over a long distance requires more energy compared to local storage. Research from 2012 claimed that 30 billion watts of electricity were used annually by cloud computing [71]. The annual energy consumption by data centers in the U.S.A. is equivalent to that of 6.4 million average houses. Optimizing and utilizing energy is a primary issue with cloud computing. This also serves as an inspiration for green cloud computing. Many blockchain techniques rely on a proof-of-work consensus mechanism to validate transactions, as complex computations consume a lot of power from the participating machines. Blockchain depends on hundreds of miners using heavy electric power equipment to validate and add transactions. The amount of energy that is consumed depends on how many miners are working. As a result, 204.5 terawatt-hours of electricity are used by blockchain alone each year. At present, Bitcoin consumes approximately 150 terawatt-hours of electricity annually, which is more than the consumption of Argentina, with a population of 45 million [72].

##### 4.5.2. Dependency on Other Tools

As blockchain technology is still in an early stage, most of its associated systems have infrastructure issues. The current methods used for development, testing, and performance evaluation raise questions regarding their decentralized characteristics due to their dependency on third-party tools and technologies. Due to the use of third-party storage, insurance companies and data-owners are still hesitant to trust in the data security and privacy provided by cloud computing and blockchain.

##### 4.5.3. Scalability

Scalability issues have emerged with the increasing numbers of nodes and transactions in blockchain. This issue is common in public blockchain applications, since each node must store data and perform computations to validate each transaction. Therefore, public blockchains always require a large amount of storage space, low latency, and a lot of computational power.

#### 4.5.4. Lack of Definitions and Standards

Major cloud service providers have started to release their own cloud computing products or solutions. There are no unambiguous technical standards for cloud computing at present, despite the fact that its definition and range of applications are constantly expanding. There are no suitable laws or rules for insurance companies. This includes the absence of insurance policies and transmission criteria for accident videos. As a result of this shortage, further complications and problems may arise, as well as legal, social, and ethical concerns, especially when working with sensitive data that might present ethical challenges.

### 5. Potential Solutions Regarding Challenges in Cloud- and Blockchain-Based Insurance Systems

In the previous section, we highlighted the key problems and challenges related to cloud- and blockchain-based auto-insurance systems. In this section, some useful recommendations are provided to overcome these issues and problems. Figure 3 presents the aforementioned auto-insurance challenges in quarter circles, together with suitable recommendations in rectangles.

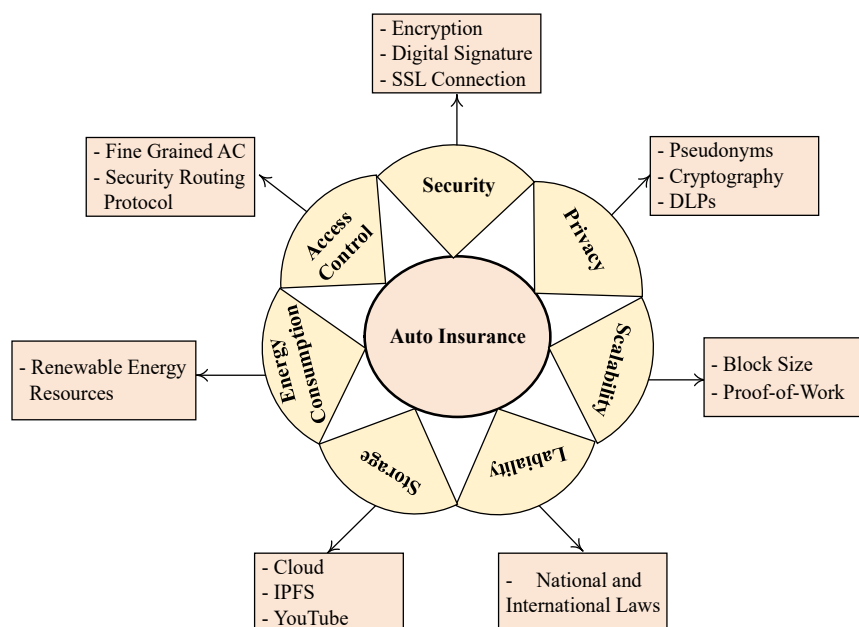


Figure 3. Auto-insurance challenges and recommendations.

#### 5.1. Confidentiality

1. It is important to ensure that data related to the accident are not disclosed. Otherwise, clients may lose confidence in their service providers. Service providers can enhance the privacy of their insurance data by combining two or more methods (for example, reversible data hiding and discrete cosine transform provide a strong encryption algorithm in the encrypted domain [43,44], along with public-private key encryption with a secret sharing scheme).
2. It is preferable to secure data by employing a robust encryption method, especially before storing the data in the cloud.
3. Off-chain transactions between users and the server can be protected using timestamps, an authentic user token, or a private key [42].
4. Cryptography and signature generation techniques can be used in blockchain to ensure confidentiality. The use of distributed ledgers for trusted authentication, public key encryption using Cecoin distribution, etc., for security purposes have already been investigated in the literature [57].

5. It is also important to develop a scalable, AI-based privacy approach that can handle all privacy-related (confidentiality) issues.

#### 5.2. Integrity/Immutability

1. The immutable ledger can be used to ensure data integrity [73], as any kind of modification to the data or information requires the consensus of the network members [74].
2. Digital signatures can be used to preserve network integrity in public key encryption methods.
3. One should avoid storing blockchain keys on one's computer or mobile device as text files.
4. Routine system assessments should be performed and nodes, applications, processes, accessed devices, and their behavior should be monitored.
5. Blockchain can be used to store important information, such as the hash values of multimedia files or information regarding the history of system access and message exchanges.
6. Modifications require network member consensus.

#### 5.3. Availability

1. To ensure the consistency and availability of shared data, blockchain uses a consensus mechanism. The liveness attribute of a consensus method in blockchain ensures that all consensus rounds are completed. Even if an agreement could not be reached, the consensus mechanism should not be left inactive indefinitely to ensure its availability. The consensus mechanisms are designed to ensure that all participants are in the same state following a consensus round, ensuring consistency. It is crucial to remember that enough research is being conducted to strengthen network architectures and guarantee that transactions are recorded in blockchains in a way that preserves their secrecy, integrity, and privacy [75].
2. Source authentication and encryption can be utilized to solve issues with an accident video's confidentiality, availability, and integrity.
3. The following guidelines should be used to prevent cyber-attacks [65].
  - Avoid saving keys/passwords as text files on a PC or mobile device.
  - Boost browser security by adding a trusted add-on that alerts you to potentially dangerous and harmful websites.
  - Increase device security by installing reputable antivirus software and malicious-link-detecting tools.
  - Open only trusted hyperlinks. If you receive an email asking for login information regarding the problem, verify it before opening.
  - Do not use open Wi-Fi networks while performing certain critical or financial operations.

#### 5.4. Privacy

1. In a blockchain, privacy is protected with a variety of measures, including the employment of pseudo-identities in place of genuine ones, the asymmetric encryption of transaction data, and the use of proxy re-encryption technology when looking up a vehicle's history [76]. With this approach, data exchanges between several authorities ensure data privacy. Therefore, the blockchain-based auto-insurance system has a high level of secrecy compared to other competitors.
2. Improved security algorithms and lightweight security schemes are essential to reducing the response time. A balance must be obtained between security protection and cost, as effective security protection and procedures require substantial processing and transmission costs.
3. The security system must be scalable to manage the ever-changing number of vehicles with respect to their positions. Regular and unusual traffic, such as the large volumes of traffic generated by special events, should be handled by security mechanisms.

4. To remain anonymous, a pseudonym can be used to replace the vehicle identification number. After a certain period of time, the pseudonym should expire. After the previous alias expires, a new one will be assigned, i.e, it must be updated on a regular basis.
5. Digital license plates or electronic license plates, which are wireless devices that broadcast a unique identifying string on a regular basis, have been offered as solutions. Temporary public keys can be used as digital license plates to protect privacy while allowing for wireless broadcasts [77].
6. It is important to determine the cryptographic techniques used for block verification and writing, authentication techniques, digital certificates, and transaction signatures. It is preferable to encrypt any keys associated with video data or third-party storage. In the event that encryption fails to protect data from attacks, data access must be monitored (or machine learning tools must be used) to track unusual data access patterns.

#### 5.5. Access Control

1. It is important to ensure that the cloud service provider or its employees do not have access to client information or other information related to insurance. Therefore, it is preferable to use fine-grained access control at the trusted authority level by integrating the blockchain with the control system and data [69].
2. To prevent network attacks (especially routing attacks), secure routing protocols should be implemented (with certificates), data should be encrypted, and secure passwords should be used and updated frequently.

#### 5.6. Storage

1. Alternative off-chain data storage is required for various blockchain-compatible applications. However, a lack of access control is a key issue with these systems, especially if they are used in operational and sensitive areas, such as the financial sector. Each block in the blockchain is interlinked to the one before it, making it hard to change the data that are contained, because editing every previous block and its replications is impossible.
2. Additionally, the stored data are protected with a digital signature based on hash functions, as well as a time and date stamp. Any effort to tamper with the data will be detected, because the new digital signature will be different to the old one. The stored data will become immutable and transparent as a result of the interconnection of the hash values of the consecutive blocks.

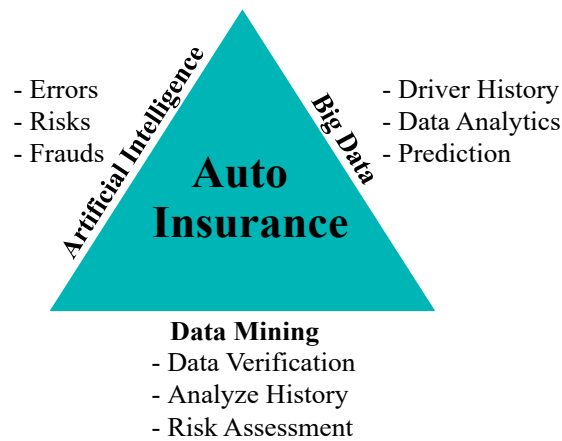
#### 5.7. Other Challenges

1. The energy problem can be solved by adopting measures such as renewable energy sources, using the heat generated by computer servers for other purposes, and shutting down hardware that is no longer functional [71].
2. An efficient task-scheduling algorithm should be used for the efficient utilization of resources, avoiding resources that consume energy and have no assigned task.
3. To increase user trust in the case of a dependent tool, control over the data should be given to their owner. To prevent malicious attackers, it is important to encrypt insurance-related data, including accident videos and other relevant information.
4. Many other solutions, such as proof-of-work and block size, can be used to deal with blockchain scalability [78].
5. Laws such as the GDPR need to be implemented worldwide. According to the GDPR passed by the European Parliament in 2016, which took effect in 2018, organizations must not process personal data unless they satisfy all legal criteria and state regulations [62]. The GDPR codified the updated and unified data privacy rules of the European Union.

## 6. Future Research Directions

Researchers, practitioners, and business experts are always looking for better and more innovative ways to transform the conventional auto-insurance industry into a modern one. They are transforming the entire infrastructure by implementing new and innovative technologies to enhance security, privacy, data management, and storage. In Sections 4 and 5, we discussed the potential issues and possible solutions to these challenges. In the current section, we discuss possible future research directions.

1. No fully reliable methods and frameworks have been proposed or implemented to date for cloud- or blockchain-based auto-insurance systems to ensure the availability of the necessary forensic data. The absence of a reliable dataset can lead to incorrect decisions [27]. Therefore, more research is required from both researchers and insurance organizations to ensure the complete availability of these data without any loss of information.
2. Data security and privacy are key concerns in the auto-insurance sector. “Cloud services lack data security” [79]: compared to cloud computing, blockchain technology offers the opportunity to provide secure data transformation using public and private key encryption. Due to the immutable nature of blockchain technology, blockchain-based data exchange can save an insurer the expense of obtaining a public data subscription to reduce fraud. Kishor et al., in [79], mentioned that “implementing blockchain will make data more secure”. Moreover, the study presented in [69] proved that blockchain has the potential to deal with all possible privacy-related threats. More research by academics and insurance firms based on simulations is needed to ensure safe communication in the insurance sector.
3. It is necessary to study and investigate the data storage problem, particularly in blockchain, because data accessibility depends on both private and shared storage. Permanent data storage on every block and the exponential increase in size are the main reasons for the scalability issue [74]; researchers have a responsibility to ensure that a significant amount of secure storage can be provided.
4. Researchers and practitioners should focus on the development of attestation methods and procedures to ensure the precision, dependability, and integrity of the data provided by CAVs as evidence.
5. Encrypting data before storing or uploading them and creating an access policy based on user identity for decryption are standard solutions for data sharing and collaboration. If data are encrypted, they will be unusable, even if leaked to an unauthorized party. Consequently, it is important to recognize and assess the weaknesses and vulnerabilities of encryption algorithms. Increased trust in the cloud, combined with cryptographic approaches, can aid in the implementation of dependable controls, resulting in real business intelligence benefits for stakeholders. Therefore, a suitable encryption technique needs to be developed to meet the privacy requirements [69].
6. AI, big data, and data-mining techniques can be applied to auto-insurance to handle the various associated challenges, as illustrated in Figure 4. These can be used to monitor user activity in the auto-insurance sector and to keep track of stored data. Auto-insurance companies can benefit from AI by reducing process errors, predicting risks, and identifying fraud [26]. Because of this, the insurance provider will be better able to recommend insurance to customers based on their needs. Consumers can also benefit from enhanced AI-based claims processing. Auto-insurance companies can exploit big data in a variety of ways. For example, telematics provides insurers with the ability to collect information about driver usage and behavior to offer usage-based insurance and premium discounts. Auto-insurance firms can be protected from many types of fraud using big data [27]. For example, prediction models can be used to compare an individual’s information to previous fraudulent profiles, facilitating further investigation. ML approaches enable insurers to verify the captured data and conduct more accurate risk assessments by analyzing the potential client’s past behavior and the behavior of other clients with similar demographic characteristics.



**Figure 4.** Emerging technologies in auto-insurance.

7. Automotive forensics aims to generate data to aid in criminal prosecutions, accident investigations, and root cause analyses. For example, a digital forensic system can be created that compares the analysis results with video records to determine drivers' responsibility for accidents using percentages (e.g., driver A is 90% responsible, and driver B 10%). This system could identify critical aspects of an accident video, guiding the decision regarding the percentages. After examining a video of a newly submitted crash, the system provides human inspectors with a predicted percentage of responsibility for each driver and the decisive moments in the video so they can make quick and accurate decisions.
8. In digital forensic investigations conducted by insurance companies, blockchain can be used for evidence collection, archiving, evidence validation, and analysis. Blockchain is a better option, as it allows for records to be traceable as well as immutable. The development of and advances in forensic techniques require the various challenges in existing forensic techniques to be overcome.
9. It is important to improve the legal and regulatory environment so that the access to data is in the best interest of both consumers and insurance companies, maintaining privacy. A comprehensive international legal framework is needed because each country's electronic and cyber footprints change over time. Therefore, investigators need to follow formal procedures, in accordance with local laws and standards, to ensure the integrity of the obtained evidence.

From the above discussion, it can be seen that several potential solutions exist that use AI, blockchain, and cloud computing to resolve the various challenges related to auto-insurance companies. All the challenges and their potential solutions are interrelated, and an optimal, robust, and well-established auto-insurance application requires a system based on AI, blockchain, and cloud computing. Despite the fact that cloud computing and blockchain can have security (and other) flaws, cyber-security experts can greatly mitigate these issues. Blockchain can be most safely deployed by professionals and practitioners with good analytical and technical skills. It is important to inform users and employees of the risks associated with information security.

## 7. Conclusions

The primary goals of this study were to introduce the possibility that blockchain and cloud technologies could improve the auto-insurance sector and to understand how this might work. State-of-the-art approaches to auto-insurance systems were investigated, particularly those based on cloud and blockchain technology. We analyzed, synthesized, and presented all the challenges in cloud- and blockchain-based auto-insurance systems found in the literature. Our survey provided a comprehensive overview of all the potential pitfalls in the various forms of cloud-based and blockchain-based auto-insurance. This survey highlighted issues in the auto-insurance sector using gap analysis, identified areas



for further analysis, and provided academics and practitioners with guidance for further investigations. We anticipate that this survey will provide a roadmap for the auto-insurance sector when using cloud or blockchain technologies with AI and help researchers and practitioners to identify relevant avenues of study for the future. Based on our gap analysis, we believe that it is important to set standards for digital forensics. The aforementioned issues call for several fundamental modifications to the use of digital forensics in insurance companies, as well as more concerted efforts in this area. Insurance companies' digital forensics solutions should be able to learn from usage patterns by monitoring vehicle logs and user actions and by applying advanced ML and deep learning algorithms. Digital forensics could be helpful in assessing and calculating each driver's liability in percentages, especially in multi-vehicle accidents.

In addition, data storage and security are crucial and cannot be neglected. Different sources of data, their dynamic behavior, and the lack of trust between different stakeholders are the primary challenges in the insurance industry. Therefore, cloud and blockchain technologies should be thoroughly investigated by finding security holes and ways to enhance security. Although the auto-insurance sector is still at an early stage in the adoption of these methods, there is an opportunity to make auto-insurance services more effective and efficient.

From this discussion, it is concluded that, by using cloud- and blockchain-based auto-insurance systems with technologies such as AI, big data, and IoT, insurance management could be made more efficient and insurance fraud could be detected and prevented. When an accident occurs, blockchain technology can accurately record the time, location, and other factors that can prevent insurance companies from being defrauded. AI can help with customer interactions and speed up the claims process. Big data technologies facilitate data monitoring and analysis. Blockchain and IoT can be used to track a car's operational data, driving history, and other relevant information.

**Author Contributions:** Conceptualization, A.M. and S.Y.N.; writing—original draft preparation, A.M. and A.K.; writing—review and editing, S.L. and S.Y.N.; visualization, A.M., S.L. and A.K.; funding acquisition, S.Y.N. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported in part by the National Research Foundation of Korea (NRF) through the Korean Government [Ministry of Science and ICT (MSIT)] under Grant 2020R1A2C1010366, and in part by the Basic Science Research Program through the NRF funded by the Ministry of Education under Grant 2021R1A6A1A03039493.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Singh, J. Identity Fraud's Impact on the Insurance Sector, Thomson Reuters. Available online: [/https://legal.thomsonreuters.com/en/insights/articles/identity-frauds-impact-on-the-insurance-sector](https://legal.thomsonreuters.com/en/insights/articles/identity-frauds-impact-on-the-insurance-sector) (accessed on 22 February 2023).
2. Jeyong, J.; Kim, B.J. Insurance Fraud in Korea, Its Seriousness, and Policy Implications. *Front. Public Health* **2021**, *9*, 791820. [CrossRef]
3. Reports, and Publication: Insurance Fraud, FBI. Available online: <https://www.fbi.gov/statsservices/publications/insurance-fraud>. (accessed on 16 October 2022).
4. Insurance Information News. Available online: <https://www.iii.org/article/background-on-insurance-fraud> (accessed on 23 February 2023).
5. Stijn, V.; Dedene, G. Insurance fraud: Issues and challenges. *Geneva Pap. Risk Insur. Issues Pract.* **2004**, *29*, 313–333.
6. Tillman, R. Abandoned Consumers: Deregulation and Fraud in the California Auto Insurance Industry. *Soc. Policy Soc.* **2003**, *2*, 45–53. [CrossRef]
7. Yogesh, K. AI techniques in blockchain technology for fraud detection and prevention. In *Security Engineering for Embedded and Cyber-Physical Systems*; CRC Press: Boca Raton, FL, USA, 2023; pp. 235–252.
8. Satoshi, N. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Bus. Rev.* **2008**, 21260.
9. Shrestha, R.; Bajracharya, R.; Shrestha, A.P.; Nam, S.Y. A new-type of blockchain for secure message exchange in VANET. *Digit. Commun. Netw.* **2020**, *6*, 177–186.
10. Dustin, B. Understanding Trie Databases in Ethereum. Available online: <https://medium.com/shyft-network-media/understanding-trie-databases-in-ethereum-9f03d2c3325d> (accessed on 3 January 2023).

11. Monireh, V.; HamlAbadi, K.G.; Saghiri, A.M.; Rashidi, H. A self-organized framework for insurance based on internet of things and blockchain. In Proceedings of the 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), Barcelona, Spain, 6–8 August 2018; IEEE: New York, NY, USA, 2018; pp. 169–175.
12. Lookman, S.H.; Balasubramanian, T. Survey of insurance fraud detection using data mining techniques. *arXiv* **2013**, arXiv:1309.0806.
13. Hongbing, W.S. Consumers' insurance literacy: Literature review, conceptual definition, and approach for a measurement instrument. *Eur. J. Bus. Manag.* **2019**, *11*, 49–65.
14. Dong, W.H. Research on the features of car insurance data based on machine learning. *Procedia Comput. Sci.* **2020**, *166*, 582–587.
15. Shrestha, R.; Bajracharya, R.; Shrestha, A.P.; Nam, S.Y. A survey on driving behavior analysis in usage based insurance using big data. *J. Big Data* **2019**, *6*, 86.
16. Gao, G.; Meng, S.; Wüthrich, M. V What can we learn from telematics car driving data: A survey. *Insur. Math. Econ.* **2022**, *104*, 185–199. [[CrossRef](#)]
17. Pastor, A.M. Cloud Computing Adoption in Insurance Companies in Kenya. Ph.D. Thesis, University of Nairobi, Nairobi, Kenya, 2015.
18. Afnan Ullah, K. Data Confidentiality and Risk Management in Cloud Computing. Ph.D. Thesis, University of York, York, UK, 2014.
19. Brophy, R. Blockchain and insurance: A review for operations and regulation. *J. Financ. Regul. Compliance* **2019**, *28*, 215–234. [[CrossRef](#)]
20. Amponsah, A.A.; Adekoya, A.F.; Weyori, B.A. Blockchain in Insurance: Exploratory Analysis of Prospects and Threats. *Int. J. Adv. Comput. Sci. Appl. (IJACSA)* **2021**, *12*, 120153. [[CrossRef](#)]
21. Abhinav, P.; Tiwari, C.K.; Behl, A. Blockchain technology in financial services: A comprehensive review of the literature. *J. Glob. Oper. Strateg. Sourc.* **2021**, *14*, 61–80.
22. Chen, W.; Xu, Z.; Shi, S.; Zhao, Y.; Zhao, J. A survey of blockchain applications in different domains. In Proceedings of the 2018 International Conference on Blockchain Technology and Application, Guilin, China, 10–12 December 2018; pp. 17–21.
23. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* **2020**, *107*, 841–853. [[CrossRef](#)]
24. Sharma, T.; Zhou, Z.; Miller, A.; Wang, Y. Exploring Security Practices of Smart Contract Developers. *arXiv* **2022**, arXiv:2204.11193.
25. Shaoan, X.; Zheng, Z.; Chen, W.; Wu, J.; Dai, H.-N.; Imran, M. Blockchain for cloud exchange: A survey. *Comput. Electr. Eng.* **2020**, *81*, 106526.
26. Martin, E.; Nuessle, D.; Staubli, J. The impact of artificial intelligence along the insurance value chain and on the insurability of risks. *Geneva Pap. Risk Insur. Issues Pract.* **2022**, *47*, 205–241.
27. Botond, B.; Ciumas, C.; Zsolt Nagy, B. Automobile insurance fraud detection in the age of big data—A systematic and comprehensive literature review. *J. Financ. Regul. Compliance* **2022**.
28. Rajesh, G.; Tanwar, S.; Kumar, N.; Tyagi, S. Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review. *Comput. Electr. Eng.* **2020**, *86*, 106717.
29. Gatteschi, V.; Lamberti, F.; Demartini, C.; Pranteda, C.; Santamaría, V. Blockchain and smart contracts for insurance: Is the technology mature enough? *Future Internet* **2018**, *10*, 20. [[CrossRef](#)]
30. Mehmet, D.; Turetken, O.; Ferworn, A. Blockchain based transparent vehicle insurance management. In Proceedings of the 2019 Sixth International Conference on Software Defined Systems (SDS), Rome, Italy, 10–13 June 2019; IEEE: New York, NY, USA, 2019.
31. Hoang Tam, V.; Mehedy, L.; Mohania, M.; Abebe, E. Blockchain-based data management and analytics for micro-insurance applications. In Proceedings of the 2017 ACM Conference on Information and Knowledge Management, Singapore, 6–10 November 2017; pp. 2539–2542.
32. Rui, R.; Pereira, J.L. Avoiding insurance fraud: A blockchain-based solution for the vehicle sector. *Procedia Comput. Sci.* **2019**, *164*, 211–218.
33. Oham, C.; Jurdak, R.; Kanhere, S.S.; Dorri, A.; Jha, S. B-fica: Blockchain based framework for auto-insurance claim and adjudication. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Melbourne, VIC, Australia, 6–8 December 2021; IEEE: New York, NY, USA, 2018; pp. 1171–1180.
34. Mansor, H.; Markantonakis, K.; Akram, R.N.; Mayes, K.; Gurulian, I. Log your car: The non-invasive vehicle forensics. In Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, 23–26 August 2016; IEEE: New York, NY, USA, 2016; pp. 974–982.
35. Yoon, C.; Hwang, J.; Cho, M.; Lee, B.G. Study on did application methods for blockchain-based traffic forensic data. *Appl. Sci.* **2021**, *11*, 1268. [[CrossRef](#)]
36. Oham, C.; Michelin, R.A.; Jurdak, R.; Kanhere, S.S.; Jha, S. WIDE: A witness-based data priority mechanism for vehicular forensics. *Blockchain Res. Appl.* **2022**, *3*, 100050. [[CrossRef](#)]
37. Nishara, N.; Abugabah, A. Blockchain for automotive: An insight towards the IPFS blockchain-based auto insurance sector. *Int. J. Electr. Comput. Eng. (IJECE)* **2021**, *11*, 2443–2456.

38. Bader, L.; Bürger, J.C.; Matzutt, R.; Wehrle, K. Smart contract-based car insurance policies. In Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 10–12 December 2018; IEEE: New York, NY, USA, 2018; pp. 1–7.
39. Saeedi, K.; Wali, A.; Alahmadi, D.; Babour, A.; AlQahtani, F.; AlQahtani, R.; Rabah, Z. Building a blockchain application: A show case for healthcare providers and insurance companies. In *Future Technologies Conference*; Springer: Cham, Switzerland, 2019; pp. 785–801.
40. Saldamli, G.; Reddy, V.; Bojja, K.S.; Gururaja, M.K.; Doddaveerappa, Y.; Tawalbeh, L. Health care insurance fraud detection using blockchain. In Proceedings of the 2020 Seventh International Conference on Software Defined Systems (SDS), Paris, France, 20–23 April 2020; IEEE: New York, NY, USA, 2020; pp. 145–152.
41. Khaliq, K.A.; Chughtai, O.; Shahwani, A.; Qayyum, A.; Pannek, J. Road accidents detection, data collection and data analysis using V2X communication and edge/cloud computing. *Electronics* **2019**, *8*, 896. [\[CrossRef\]](#)
42. Wan Hazimah Wan, I.; Ramadhani Mohd Husny, H.; Ya Abdullah, N.; Indit Anak Janang, C. Android Application for Car Black Box with Cloud Storage. *J. Comput. Technol. Creat. Content (JTec)* **2017**, *2*, 29–34.
43. Puteaux, P.; Puech, W. An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 1670–1681. [\[CrossRef\]](#)
44. Wen, H.; Ma, L.; Liu, L.; Huang, Y.; Chen, Z.; Li, R.; Zhang, C. High-quality restoration image encryption using DCT frequency-domain compression coding and chaos. *Sci. Rep.* **2022**, *12*, 16523. [\[CrossRef\]](#)
45. Jabar, H.Y.; Kumar Saini, D. Cloud computing and accident handling systems. *Int. J. Comput. Appl.* **2013**, *63*, 19.
46. Shradha, D.; Gadekar, P.; Labde, S.; Munde, S.; Joshi, S.G. MATCH-Mobile Auto-Insurance Claim and Help System. *Int. J. Innov. Eng. Res. Technol.* **2016**, *3*, 1–5.
47. Elmer, M.R. Centralized smart parking and insurance applications for intelligent vehicles in a smart city utilizing the cloud computing paradigm. *Int. J.* **2020**, *9*, 4. [\[CrossRef\]](#)
48. Abhijeet, C.A.; Todekar, M.N. Dependable Storage for Vehicle Insurance Management through Secured Encryption in Cloud Computing. *Glob. J. Eng. Sci. Res. Manag.* **2014**.
49. Cebe, M.; Erdin, E.; Akkaya, K.; Aksu, H.; Uluagac, S. Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles. *IEEE Commun. Mag.* **2018**, *56*, 50–57. [\[CrossRef\]](#)
50. Madhusudan, S.; Kim, S. Blockchain based intelligent vehicle data sharing framework. *arXiv* **2017**, arXiv:1708.09721.
51. Oham, C.; Michelin, R.A.; Jurdak, R.; Kanhere, S.S.; Jha, S. B-FERL: Blockchain based framework for securing smart vehicles. *Inf. Process. Manag.* **2021**, *58*, 102426. [\[CrossRef\]](#)
52. Amponsah, A.A.; Adekoya, A.F.; Weyori, B.A. Improving the Financial Security of National Health Insurance using Cloud-Based Blockchain Technology Application. *Int. J. Inf. Manag. Data Insights* **2022**, *2*, 100081. [\[CrossRef\]](#)
53. Shi, K.; Zhu, L.; Zhang, C.; Xu, L.; Gao, F. Blockchain-based multimedia sharing in vehicular social networks with privacy protection. *Multimed. Tools Appl.* **2020**, *79*, 8085–8105. [\[CrossRef\]](#)
54. Kaja, D.V.S.; Fatima, Y.; Mailewa, A.B. Data Integrity Attacks in Cloud Computing: A Review of Identifying and Protecting Techniques. *Int. J. Res. Publ. Rev.* **2022**, *3*, 713–720. [\[CrossRef\]](#)
55. Meena, S.; Daniel, E.; Vasanthi, N.A. Survey on various data integrity attacks in cloud environment and the solutions. In Proceedings of the 2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT), Nagercoil, India, 20–21 March 2013; IEEE: New York, NY, USA, 2013; pp. 1076–1081.
56. How Much Electricity Does the Cloud Use? Available online: <https://www.greenamerica.org/faq/how-much-electricity-does-cloud-use> (accessed on 4 July 2022).
57. Mohanta, B.K.; Jena, D.; Panda, S.S.; Sobhanayak, S. Blockchain technology: A survey on applications and security privacy challenges. *Internet Things* **2019**, *8*, 100107. [\[CrossRef\]](#)
58. Vimal Mani, C.I.S.A. A View of Blockchain Technology from the Information Security Radar. *ISACA J.* **2017**, *4*. Available online: <https://www.isaca.org/resources/isaca-journal/issues/2017/volume-4/a-view-of-blockchain-technology-from-the-information-security-radar> (accessed on 22 February 2023).
59. Godfrey, M.; Zulkernine, M. Preventing cache-based side-channel attacks in a cloud environment. *IEEE Trans. Cloud Comput.* **2014**, *2*, 395–408. [\[CrossRef\]](#)
60. Why the Evolution of Blockchain Reliability is Critical to Protecting Your Digital Assets. 2020. Available online: <https://www.weforum.org/agenda/2020/06/evolution-of-blockchain-reliability-and-digital-asset-protection/> (accessed on 19 July 2022).
61. EU. *Cyber Risk for Insurers: Challenges and Opportunities*; Publications Office of the European Union: Brussels, Belgium, 2019; ISBN 978-92-9473-214-9.
62. Castagna, R.; Lavery, T. General Data Protection Regulation (GDPR). Available online: <https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR> (accessed on 3 August 2022).
63. Di Francesco Maesa, D.; Mori, P.; Ricci, L. Blockchain based access control. In Proceedings of the IFIP International Conference on Distributed Applications and Interoperable Systems, Neuchatel, Switzerland, 19–22 June 2017; Springer: Cham, Switzerland, 2017; pp. 206–220.

64. Steichen, M.; Fiz, B.; Norvill, R.; Shbair, W.; State, R. Blockchain-based, decentralized access control for IPFS. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; IEEE: New York, NY, USA, 2018; pp. 1499–1506.
65. Blockchain Security Issues and How to Prevent Them. 02-16-22. Available online: <https://www.fastcompany.com/90722111/5-blockchain-security-issues-and-how-to-prevent-them> (accessed on 5 July 2022).
66. Chandrasekaran, K.; Manoj, V. Thomas, Distributed access control in cloud computing systems. *Encycl. Cloud Comput.* **2016**, 417.
67. Miltchev, S.; Smith, J.M.; Prevelakis, V.; Keromytis, A.; Ioannidis, S. Decentralized access control in distributed file systems. *ACM Comput. Surv. (CSUR)* **2008**, 40, 1–30. [[CrossRef](#)]
68. Alansari, S.; Paci, F.; Sassone, V. A distributed access control system for cloud federations. In Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 5–8 June 2017; IEEE: New York, NY, USA, 2017; pp. 2131–2136.
69. Djenouri, Y.; Yazidi, A.; Srivastava, G.; Chun-Wei Lin, J. Blockchain: Applications, Challenges, and Opportunities in Consumer Electronics. *IEEE Consum. Electron. Mag.* **2023**. [[CrossRef](#)]
70. Wang, C.; Wang, Q.; Ren, K.; Lou, W. Privacy-preserving public auditing for data storage security in cloud computing. In Proceedings of the 2010 IEEE Infocom, San Diego, CA, USA, 15–19 March 2010; IEEE: New York, NY, USA, 2010; pp. 1–9.
71. Brdar, D. Cloud Computing Energy’s Efficiency Problems. Available online: <https://www.nasdaq.com/articles/cloud-computing-energys-efficiency-problems> (accessed on 9 July 2022).
72. Feign, A. How Much Energy Does Bitcoin Use? 2021. Available online: <https://www.coindesk.com/business/2021/08/18/how-much-energy-does-bitcoin-use/> (accessed on 14 July 2022).
73. Computerweekly, Security Think Tank: Use Blockchain for Integrity and Immutability Checks. Available online: <https://www.computerweekly.com/opinion/Security-Think-Tank-Use-blockchain-for-integrity-and-immutability-checks> (accessed on 24 February 2023).
74. Ali, O.; Jaradat, A.; Kulakli, A.; Abuhalimeh, A. A comparative study: Blockchain technology utilization benefits, challenges and functionalities. *IEEE Access* **2021**, 9, 12730–12749. [[CrossRef](#)]
75. Kim, T.; Jung, I.Y.; Hu, Y.C. Automatic, location-privacy preserving dashcam video sharing using blockchain and deep learning. *Hum. Centric Comput. Inf. Sci.* **2020**, 10, 36. [[CrossRef](#)]
76. Liu, X.; Yang, H.; Li, G.; Dong, H.; Wang, Z. A blockchain-based auto insurance data sharing scheme. *Wirel. Commun. Mob. Comput.* **2021**, 2021, 3707906. [[CrossRef](#)]
77. Jinyuan, S.; Zhang, C.; Zhang, Y.; Fang, Y. An identity-based security system for user privacy in vehicular ad hoc networks. *IEEE Trans. Parallel Distrib. Syst.* **2010**, 21, 1227–1239. [[CrossRef](#)]
78. Kaur, G.; Gandhi, C. Scalability in blockchain: Challenges and solutions. In *Handbook of Research on Blockchain Technology*; Academic Press: Cambridge, MA, USA, 2020; pp. 373–406
79. Kishor, K.; Saxena, N.; Pandey, D. (Eds.) *Cloud-Based Intelligent Informative Engineering for Society 5.0*; CRC Press: Boca Raton, FL, USA, 2023.

**Disclaimer/Publisher’s Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.