Blockchain-based Authentication Systems for Secure Access Control in Autonomous Vehicles

By Dr. Toine Houttuin

Professor of Computer Science, Aarhus University, Denmark

1. Introduction

A blockchain has been designed to manage operations of drones in cooperation, while blockchain also guarantees stakeholders' involvement in U-Space governance. The blockchain-based protocol is used to ensure safe emergency message transmission in vehicular networks while providing vehicle-to-vehicle (V2V) data sharing in a secure manner. Secure and privacy-preserving message dissemination and query-based operations in vehicular networks is enabled by the state-of-the-art blockchain-based protocol. Blockchain is used to facilitate anonymous voting in IoV. A framework for Cooperative Intelligent Transport System (C-ITS) infrastructure that utilizes blockchain to secure and provide privacy at two levels, i.e. inter- and intra-coordination functionalities is proposed. It ensures secure vehicle-to-everything (V2X) communications in autonomous vehicles through blockchain.

The next phase in the development of vehicular ad-hoc networks (VANETs) comprises the proliferation of autonomous and connected vehicles. These vehicles are super-imposed by Internet-of-Things (IoT) sensors and actuators, such as Light Detection and Ranging (LIDAR), cameras, etc., to achieve better contextual awareness. The autonomous behavior of these vehicles is governed by advanced driver assistance systems (ADAS) and underlying artificial intelligent (AI) agents, that constantly learn with experience. All this infrastructure has made contemporary VANETs evolve into a more generalized framework, termed as Internet-of-Vehicles (IoV), which enables advanced vehicular services and applications [1]. Secured and reliable communication amidst IoV entities is of paramount concern for safe and efficient transportation. Therefore, many advancements are made in securing payment and communication in intelligent transportation systems (ITS) using blockchain. Intelligence through fallback stream with blockchain is resilient and immune towards regular cyber-threats associated with traditional VANETs. Due to rise in autonomous and connected vehicle portions within IoV, the automated problem detection, treatment, and deployment is necessary to ensure regular day-to-day operation. In conjunction with advances in internet of things (IoT) domain, blockchain becomes pivotal for plugging the security and privacy gaps within IoV. But, more study on blockchain platforms with respect to hardware capabilities, intensive operations, and energy efficiency is required for practical implementation within the IoV domain.

[2]

1.1. Background and Motivation

# Small cars with Level 3 or 4 autonomy are expected to be available to consumers during the second half of 2020s. Due to the growing importance of autonomous vehicles (AVs) in the future of traffic, researchers are analyzing the kinks and potential security threats brought by these emerging technologies. <br> [3] (Wor bold as well) proposed Blockchain-based cryptographic authentication for AVs utilizing ZeroKnowledge Proof-(ZKP)-based authentication for secured AV application communication. Since the Trust-From-Scratch-(TFS) issue arises during initial trust establishment, Blockchain has been proposed to provide this whole proof simplifying this into a single verification (one-shot) problem. Inter-node IoT (sensors) were considered to form trust for creating V2I communication. By the same authors, additional design for off-chain TFS (TC) is suggested for realizing AV platooning with the tangle (IoT directed acyclic graph). AV-based services have been extensively discussed from the communication and application perspectives.[4] security is extremely important in advanced computing including AVs. The scenarios being on one hand highly connected and being on the other hand AD (semi/full) equipped are not answering for the standard computer and hardware security tasks. In the connected transportation and communication locations, the security features are very strongly required by the multi-digit authentication rights form signing for example: strong psycho-metrics (biometric, author, only password, etc.) between V2X links, via an IoT-type connection of the (IoT: Internet of Things) motor vehicles. These access points (APs) can be equipped with personalized equipment, so that motor vehicles can connect securely to these endpoints through uniquely manufacturer or agent approved access points with a secure connection under the right of exclusive or settlement. To form secure access and a pre-trusted environment, it would allow a vehicle

manufacturer or its professional partner to design, install, and then establish a digital certificate environment.

1.2. Research Objectives

In this work, we are concerned with the authentication mechanisms of autonomous vehicles based on blockchain technology. Multi-level trust management and vehicle data security and privacy are the main objects of our research. [5] The aims of this work can be summarized as follows: identity safely and efficiently; securely share data stored inside vehicles; vehicle and IoT device lightweight authentication; multi-PKI and multi-TA traffic authority authentication; improving the efficiency of the authentication mechanism in terms of the time required to authenticate a communication entity.

Blockchain-based authentication systems, which provide secure access to autonomous vehicles, are addressed in this work. In the contexts of safety message dissemination, secure vehicle-to-vehicle data sharing, privacy-friendly multi-TA traffic authority authentication and anonymous voting, a blockchain-based protocol is proposed to address security concerns in autonomous vehicles. [6] By providing efficient identity management this protocol aims at facilitating secure drone communication, secure emergency message relay, secure vehicle-to-vehicle communication, secure vehicle-to-infrastructure communication, secure data storage with fine-grained access policies, and facilitate a privacy-friendly Coop-erative Intelligent Transport Systems (C-ITS) by offering anonymous voting. The protocol is deployed on top of public blockchains.

1.3. Scope and Limitations

One of the promising opportunities provided by blockchain technology is enabling vehicle-to-everything communication systems to implement privacy-preserving schemes in the creation and management of the shared entities. However, the analysis of the possible strategies and the investigation of their implications in autonomous vehicles has not yet been carried out in specific and feasible directions within the context of blockchain technologies. Additionally, blockchain-based methods to transfer securely all these pieces of information only for the intended recipient in autonomous vehicles are still underdeveloped and are very difficult to adapt for real-world deployments.

Blockchain technologies have emerged as promising alternatives to enabled data authentication and verification services in various smart and autonomous research fields [7]. In the context of autonomous vehicles, blockchain technologies offer new solutions to enhance security, increase privacy, optimize functionalities, improve data storage, and support interactions between interconnected vehicles and their infrastructure [1]. For instance, blockchain technologies can be used to provide unforgeable and transparent mechanisms for secure key management, communications with privacy-preserving properties, and real-time access control services in smart city scenarios [5].

2. Autonomous Vehicles and Access Control

Contrary to the queueing intermezzo of Chapter 9, the following section brings human mobility into focus. One implication of (this section) is that it is policy and people who are driving the future of Urban Mobility (UM). Traffic is an inherent part of living in a city. The transportation of people and goods is an integral part of a functioning society, now as in the past [8].

The future of urban mobility is projected to realize widespread adoptions of autonomous and ecofriendly vehicles [6]. By investigating the current stage of Autonomous Vehicle (AV) technology, an AV's benefit to society, and its challenges, one may want to discard the term 'autonomous'. However, a set of PM invited, were asked by the AV company's co-founders to define the believers' version of an AV. No surprise that this group "piled into the back of a truck." Several diverse detailed case studies are presented of the unpredictability of human behavior across different levels of various societies. Since "we can tell them apart by the accidents they cause," often, it is claimed, "AI will save us." The results of countless experiments are scrutinized to three different ends [4].

2.1. Overview of Autonomous Vehicles

Cyber-Physical System (CPS) technology is defined as the new method for developing software that innovates in the automotive space by combining the advantages of both software and hardware [9]. These are smart, state-of-the-art, complex systems that make use of the integrated technologies of the physical world, computer systems, IT, and open software and that establish the engineering of a new environment by interlocking physical processes with software processes with the development of automatic control of the transportation system [10]. The working group which uses these advancements to ensure the security of vehicle communication infrastructure, and autonomous automotive software systems, has ever more complicated software-based operations. It has been difficult to find effective security measures and to apply these to autonomous vehicles. To adopt effective measures to safely, and freely access the software system which has been developed for Autonomous Ground Vehicles [3].

2.2. Challenges in Access Control

Challenges: 1. System Efficiency: In the construction of blockchain-based mutual authentication mechanisms, how to reduce the system overhead and establish a feasible and efficient convergence process is a challenging issue, Especially in a large-scale city environment, the overhead of sensing tasks and user interactions is often heavier. 2. The Issue With Trust: Urban smart mobility combines the development trends of the Internet of Vehicles (IoV), data-driven transportation infrastructure, and the social infrastructure of modern cities. [11] Through edge computing, edge police can help AVs detect malicious behaviors of drivers and vehicles, including unexpected, aggressive vehicle operations, to enhance vehicle security. But as more communication and interactions occur, the trust demand of transportation-related sensing data gradually rises, and the trustworthiness of context data from IoV participants affects the execution of rational IOV services. In the IoV, the issue with trust has constantly been attracting extensive consideration, since V2X participants are usually not trusted each other before.

[12] [13]In a blockchain-based traffic management system, AVs can trust the spatial information from the shared map on the blockchain and make authentication decisions based on the location information on the roads. However, the spatial information shared on the blockchain cannot be tampered by the λ users; intelligent attackers may consider using dummy nodes to deceive the AVs. To address this challenge, a side-channel attack-resilient map sharing strategy has been proposed to ensure the correctness of the shared p2p geometry map, which utilizes the characteristics of usages of AVs in road scenes. In addition, blockchain-assisted intelligent transportation is conducive to the realization of urban registration area sharing and the rational censorship of illegal vehicles, since all public users can easily supervise local governments through the blockchain. Moreover, complex and detailed legitimate operation permissions in traffic configuration services of an intersection,

such as different period business opening, can be automatically realized through smart contracts on the blockchain, benefiting traffic police enforcement in the regions wherein AVs drive.

3. Blockchain Technology

[5] The vehicle is an important source of data for vehicle network systems. The vehicle digital key switching mechanism based on BIN technology adds convenience to the vehicle owner, drivers and passengers. Blockchain technology can provide a safe and trustworthy audit trail for vehicle security. When digital keys are sharable for vehicle operation collision avoidance, the concept is applied to BINs (VKEY) as a shared transaction mechanism. This configuration of blockchain technology can apply the safety protection application of digital keys to a car. Permissioned blockchain is used for pass through blockchain mechanism (PTBM) and public blockchains is based on enable vehicle shared key use without additional intervention owner of vehicle.[10] In the recent decades, few studies conducted on the blockchain approach of combining with the internet of vehicles. Blockchain technology provides an efficient solution for configuring a blockchain network that is presented in this survey. The straightforward way to use such a blockchain approach is to implement a public blockchain with an ice age protocol, but this has the disadvantages of high default delay cost and a high number of nodes making demand restrict small. Here, a multi-level architecture blockchain combines with a vehicle-to-vehicle architecture network to be studied as a private blockchain on logical separation.\Eloquent information to illicit unsuspecting hosts in reconnaissance in public blockchains. The cooperation level blockchain information is a synthetic recognition level that the permissioned blockchain can block.CONNECT intra-blockchain with recognition-enhanced VANET (ReVANET) to Release the incurred able to guide scheme.

3.1. Fundamentals of Blockchain

Data in data networks are commonly distributed, and to manage and share these data in a secure manner, the blockchain-based technologies are proposed by using record of data. Blockchain technology ensures the authenticity of vehicular transactions [14]. A unique cryptographic algorithm allows peers in vehicles to come to a consensus where they can decide to collaborate or not, which is achieved using a public ledger where all the records of transactions are stored. The algorithms to decide whether the user follows a set of rules or not are set up in blockchain-based security frameworks. Blockchain can be thought of as a moving or dynamic ledger system. This is the core property of blockchain and this property of blockchain makes it truly popular in the field of secure trusted sharing and collaborating platforms and transaction and in storage and medium comfortable. A unique transaction coupling message authentication message transmission system limits a vehicle-to-vehicle communication to be more secure and private prove with a higher comfort level. Depending on the application and the purpose or the strategy to secure the system, some of the combinations of frameworks of blockchains can be used, however, real world of autonomous driving technology are not really secure and private as most important security and privacy aspects are still open with modern blockchain-based architectures [11].

Blockchain technology was conceptualized by its creator as "an electronic means of transferring titles to real property". The fundamental concept can be seen in that statement itself - a digital ledger that verifies and records electronic transactions, ensuring data integrity and the authenticity of transaction participants [15]. Secure and transparent record-keeping enables various applications to be built with blockchain as a backend, including supply chain management, digital currencies, healthcare systems, digital democracy, voting and many more use cases. All the above applications use blockchain as a data storing system, limiting its use. Blockchain is based on peer-to-peer (P2P) decentralized algorithms that are actively involved in different domains such as a smart mobility system, a smart grid, healthcare & life sciences, and Internet of Things (IoT). Blockchain-based architectures usually consist of block storing, peer to peer distributed storage, consensus derivation, trust score processors (popularly known as miners), and independent validators. These peers basically exchange data with one another using a public blockchain network like Bitcoin and Ethereum. To secure digital transaction and guarantee the security of transactions of autonomous vehicles, the algorithms allowing or disallowing certain users from interacting with others, as in blockchain-based security framework, are set up.

3.2. Key Features for Authentication Systems

The single sign-on (SSO), which simplifies the user access to the resources, is commonly vulnerable to different types of attacks. Blockchain-based SSO and MFA are the promising trends for the IV. In the V2V technical report of the European Telecommunication Standards Institute a blockchain-distributed selection and authentication method is suggested. A blockchain-based short-range communication ETSI standard for the connected vehicles in the

5G network is copresented with an MFA system in. The system addresses three main types of IDoT attacks: authentication, audit and integrity attacks. A blockchain-based secure IoV architecture for smart transportation environments and a smart car management system in an IoV with blockchain are proposed in [8, 4]. Another Application Block-chain Vehicle Advertisement system with authentication system is running in. Yet more negative side, public blockchains offer only partial privacy since they store transaction data in an open and verifiable manner. Homomorphic encryption for the fine granular protection of user's data is designed in. In Car2Car-Transfer, the beacon system issues and transfers sensitive data in the VIN information system of a car in a way that is independent of the manufacturer.

MFA is an authentication scheme that demands multiple credentials from the user to verify his identity before granting access to the protected resources. It increases the security of the systems and it can provide an adequate defence mechanism against the brute force, dictionary, phishing, and key-logging-based cyber attacks. Today, the authentication and access control in the Internet of Vehicles are faced with considerable threats, vulnerabilities, and challenges [6]. The main challenges of the security in IV are the dynamic and large constellation of connected vehicles and applications that need to be managed in a decentralized manner, trust itself, performance, privacy, and the choice and design of secure consensus, which will lead to highly efficient authentication infrastructure. Decentralization and transparent trust mechanisms, which is offered by the blockchain technology, is widely utilized by many protocols to establish a more secure and distributed environment for security and privacy. In, the authors present a multi-factor authentication model that adopts the blockchain technology to establish a trust mechanism in the cloud-enabled Internet of Vehicles and enhance the security level.

4. Related Work

The adoption of blockchain into the vehicular platooning system is enhanced by vehicle-to-everything (V2X) using remote vehicle operations and connecting vehicles and communicative with digital platooning technology. Furthermore, evaluated through the analysis of his public key and processing of his biometrics, card approval enables valid requests regarding the obligations linked to the automobile of the driver. In the following, a request for time stamps and the unique details of the vehicle are sent to the controller of the platoon. If the confirmation code matches the flood, access to the platoon is achieved. If more than 3 consecutive login attempts go beyond, the vehicle unolean the route and transfer the route to the token-predominate validation subsequent to a safety evaluation. Many of the state-of-the-art auto-vehicle-vehicle interactions for V2X are exploited for velocity, safety, and commodity identification.

A wide range of privacy and the security mechanisms has been proposed that help IoT significantly. Some mechanisms improve the security and interact directly with blockchain [16]. In the article the security of software-defined networks and communications is examined and tested by employing blockchain. Blockchain-based authentication security issues for the vehicle network in IoT are examined in terms of environmental friendliness, driver safety, and comfortableness [10]. V2V and V2I we have improved data and standard privacy measures for information transfer. The focus here is that, without settlement models, we are designing a novel authentication mechanism that gives speed, strength, and energy efficiencieshown in the scheme's experimental results. Moreover the user's location is not revealed to anyone. All domain users are subject to verifying biometric authentication processes for better consumer safety.

4.1. Existing Authentication Systems in Autonomous Vehicles

In this section, we first introduce the structure and task done in the existing system. The system present in the three modules named as Ownership Life Achieving Module, Communication Module and Pseudonym Management Module to achieve more efficient and secure characteristics. Then, it will consist of a further module to preserve the privacy information by secure vehicle management. All the modules have personal use cases of their working scenario in containing with the blockchain network. The block is mainly divided into different elements, where paired consensus and pseudonym communication approach have been performed. And existing blocks in the data are first privacy protected and then shared among them. The entire overview of the block is clearly shown, and each module's impact on the other vital scenario was illustrated. Consider the proposed block will secure policy privacy system secure and adopt V2X communication transfer mechanisms. All the remaining modules were designed regarding the pending score at their place, where other case study titles were explained inside the other incentive as in where the real case studies will present importance [16].

Privacy Concerns unmasked in Autonomous vehicles(new) With the recent advancement in technology, the traditional cybersecurity methods have become weak to defend against the malicious attacks that compromise the system. These conventional methods cannot be extended to the autonomous vehicles, as they will become more complex and more advanced. The autonomous vehicles can handle various unexpected traffic and can work smart on behalf of the human driver and act on the given surrounding information effectively. But considering the privacy concern of the driver and the trusted entities owners, the trust among the autonomous vehicles is the main factor that needs to be considered in decentralized manner. As a way to make included trust security fallback, recent research has shared our mental resources to allow attackers to takeover and control the functionalities of the vehicle A trust based privacy controlling policy will make sure the resource management fist does no harm to the users and trust entities. It cannot identify only the malicious entity but also can enhance the ownership level of the entire system [17]. It secures the external and internal interaction module and the monitoring block both privacy and non-private data source system.

5. Proposed Blockchain-based Authentication System

Under this architecture, vehicle nodes interact with road-side units (RSUs) through V2I communication and with each other through V2V communication. We have proposed a blockchain-based V2V (B-V2V) authenticated and secure access control protocol in the literature [18]. A similar approach is presented in [19] where communication of vehicle nodes with the base station is considered along with RSUs. In the authentication mechanism, all vehicle nodes register themselves by sharing their current location-based unique IDs (IDs) randomly generated using hash-chaining values with RSUs. Once a vehicle node registers itself with the RSU, the vehicle will be notified by the RSU to create a pairwise symmetric key. All vehicle nodes perform Elliptic Curve Di$e-Hellman (ECDH) key exchange, using which the security group key will be generated. All the vehicle nodes performing ECDH should store their pairwise symmetric security group keys in their identity block.

[2] The proposed blockchain-based authentication system is used along with vehicle-to-vehicle (V2V) communication, vehicle-to-infrastructure (V2I) communication. This system will help in securely authenticating the vehicles along with secure access control for enabling vehicle-to-vehicle and vehicle-to-infrastructure communication. Attachment 1 represents the

proposed blockchain-based authentication system architecture, as it is shown in digraph viz model in attachment 1.

5.1. System Architecture

The blockchain performs anonymity without authorities and is very fault-tolerant and secure. The blockchain is also used for identity management and decentralized policy enforcement with smart contracts and demo version written in Solidity. The confidential data involved in the vehicle identity and the physical and software sensors can be secured by the use of confidentiality techniques in conjunction with RL-based Secure communication which accounts for identity affirmation verification. The Ethereum simulator has been used and performance benchmarks were analysed by Open Box. So, resulting in the proposal of a further access control application model for real-time driving scenarios for the IoV of the future [14]. All these mentioned frameworks or models are developed to improve the secure communication systems in order to take the trust to the next level and to be ready for cloud-based connected cars for a change.

The authors of [17] stated that blockchain can be leveraged for use cases that require a high level of trust. The blockchain for Identity and Access Management (IAM) in a V2X ecosystem is a major challenge. Blockchain enable vehicles that wants to communicate to proof their identity on a decentralized matter. Blockchain-based IAM in IoV can offer the possibility to manage identities and permissions when exchanging information, create new transactions among existing permissions, create an audit log for permissions, and secure personal data. Finally, a permission granting answer is issued having a real-time or O(1) complexity. A blockchain-based authentication solution in which vehicles issue credentialssigned by the blockchain platform is proposed for this paper. The issuance cost for aggregate credentials is O(n) with n the number of credentials because this process can be done by the blockchain platform off-chain. Therefore, the protocol has constant-time complexity O(1).

5.2. Authentication Process Flow

[12] An authenticated vehicle system will add security to the protocol and will prevent any unauthorized access from attacking the network. Each vehicle in the Intelligent Transportation System (ITS)/smart transportation system is considered as an independent participant in the network, and it needs to be authenticated before it takes part in the network

and accesses the transaction history of any participant. An Authentication and Authorization System (AAS) verifies the authenticity of each vehicle and provides a verification certificate for all interactions. The authentication flow is divided into two processes of initial authentication and normal authentication.[7] First, each vehicle is registered with the proposed authentication service, as shown in Figure 5 which is used to generate the credentials, and it is broadcasted into the blockchain network as connected peers. If the user vehicle is allowed to become a participant, it will be included as a peer in a blockchain network. In each connected vehicle, an identity alias and address were generated, and both of them were stored in an association table with the same primary key in order to create a connection. The vehicle has an integral role in validation and checking of the allocated certificates for reliability and credentials. This process will avoid the double entries of the vehicles as peers. The ad-hoc based distributed data exchange service can be a vehicle-to-vehicle communication to exchange the data through the-virtual channel.

6. Evaluation and Performance Analysis

[10] Security assessment of a system is always an indispensable phase in evaluating the effectiveness of any security measures. The detailed security evaluation results of the proposed system for practical implementations are discussed in this section. The results are compared with those existing schemes. In the proposed system, all the evaluation parameters are discussed viz. Efficiency analysis, Security analysis, implementation scenario and other required merits of the proposed scheme. The comparison section provides all the detailed comparison parameters and evaluation among the existing schemes [20].[12] The Smart Contracts application is evaluated using Ethereum testnet to measure the time taken for smart contract creation and to compare the gas consumed with the existing SC to evaluate by deploying the smart contract using Remix on the Remix Ethereum tool. As shown in the table, since the contract execution depends on the blockchain interaction, speed decreases rapidly as the consensus algorithm scales . Security is the In technology and transmission that prevents an attacker from tampering, disrupting, or eavesdropping on exchanged messages in a network or transaction raise. It improves the ability to keep away misinformation, corrupt information, and other illegal access. Performance is an important attribute for describing organizational environment, new development opportunities and improving in products and services. The robustness of the system according to high reliability in case of a failure is highly achieved. In the sea of researches, IoT and blockchain are-awaited growth to the front line.

Blockchain authentication is a mechanism that secures the communication between participating entities. After all of the participating network entities performing mutual authentication, the previously unknown party's identity is disclosed. Mutual authentication and distributed usage of trust relationship are two distinct security tools. Blockchain-based authentication in the IoT primarily defends the communication among IoT devices, authentication among participants in the IoT. Cross-blockchain infrastructures have been investigated, as well as the logging of Trusted Platform Module reports into a blockchain. Identity Management for IoT, Blockchain and Access Control Systems and Fair Secure Off-BlockChain Transactions and Access Policies for Enhancing Trusted Internet of Things. Cross-blockchain infrastructures have been investigated, as well as the logging of Trusted Platform Module reports into a blockchain. Identity Management for IoT, Blockchain and Access Control Systems and Fair Secure Off-BlockChain Transactions and Access Policies for Enhancing Trusted Internet of Things.

6.1. Metrics for Evaluation

[1] The future potential use-cases of blockchain in autonomous vehicle networks scenario implies that the security features of this Technology must be carefully considered. The use of blockchain at the initiative of secure applications directly impacts the security design of these applications. The blockchain can become a reference of trust. The main objective of this use-case is to position blockchain in direct authentication in order to secure devices, to demonstrate that public roads are safely shared only by devices authorized to do so; in a second way, to defend ourselves against identifying attacks that have serious consequences on the e-privacy of travelers.[10] Several security and privacy threats can occur in IoV and VANETs due to their open environment and wide range of security requirements. The blockchain is an emerging technology that can effectively secure these Information Technology (IT) systems by providing high security and privacy. This paper provides a comprehensive overview of blockchain-based authentication schemes for IoV networks and categorizes different schemes according to their betterment area, such as authentication data structure, security extensions, related technology and related security issues. The aim of this survey is to provide many open issues and future research motives to the researchers working in the fields of blockchain-based authentication methods for IoV networks providing V2V and V2X communications.

6.2. Comparison with Existing Systems

[10] Several of the proposed schemes have aimed to address security and privacy issues, yet they often become vulnerable to security and privacy threats that were not initially considered. The authors studied the security threats and challenges in existing smart city technologies and authentication mechanisms. There is a need to safeguard these systems from various types of attacks such as privacy breach, application intrusion, and service-law effect attacks. This proposed a blockchain-based radio frequency identification system which has helped to incorporate the desired anonymity levels. This is recorded in a public ledger ensuring a highly secure, unalterable, and transparent system that assures the authenticity of each vehicle on the road.[8] Blockchain technology has emerged as an effective solution to several security and privacy concerns of IoV, VANETs, and other connected and autonomous vehicles (CAV) technologies. A secured and trustable environment is essential for the functioning of all IoV components. In CAV networks, the data exchanged between the vehicles, infrastructure, and CAV applications need to be authentic and trustworthy at all times. A comprehensive survey by Junejo et al. provides comprehensive details about IoV technologies along with unique capabilities, their integrated services, and blockchain technology. Several types of data exchange and sharing scenarios have been discussed. Privacy and security aspects are discussed at different layers, i.e., V2I, I2V, and V2V. The work also surveyed multiple blockchain-like technologies (Tangle etc.) that provide the same functionality as blockchain.

7. Security and Privacy Considerations

Trading privacy for security and accessibility leads to new challenges that entail a clean-sheet approach to road related infrastructure and a break from the traditional transportation system. It is still under debate if decentralized or centralized road user identification is preferable. It is therefore essential that each vehicle is assigned a unique decentralized identifier (DID) for their lifespan, and possessed cryptographic keys, issued by a trustful authority, are sustainable even if the specific infrastructure they belong would become abolished [6]. As sensors, e.g., ultrasonic or radio frequency devices for distance measurement, and onboard-cameras and radars for environmental mapping are already proved to have false positive and negative detection rates, the accuracy of their contributions to decision making must be regularly confirmed to be processed by the SV. Furthermore, conventional road management activities, e.g., patent rights, payment to road infrastructure managing companies in case of toll roads, must be reengineered in a way which allows DIDs to make the automatic right-of-way decision.

Access control, privacy, and security are three of the first issues organizations consider when contemplating moving a workload to the cloud. These concerns are of particular urgency for smart transport systems, such as autonomous vehicles (AVs) which will not only belong to the cloud environment but be obliged to share the same road infrastructure and right-of-way with current traffic. Thanks to the Internet of Things (IoT) and the next, 5G mobile communication generation, connected and automated vehicles generate and exchange huge amounts of data every second, in real-time [12]. This information reveals unexpected insights into the driving tactics and instable environmental conditions that cannot be captured by traditional technologies. It is already known that road-side cameras categorizing pedestrians and vehicles, tracking accidents, or monitoring speed limits can be attacked by adversary traffic analysis, and speech recognition from e.g., user's smartphone can be deceived by unwanted personas. It is likely that such physical and privacy threats will even grow when billions of IoT devices contribute to smart transport and smart city traffic planning.

7.1. Threat Models

[3] In this paper the authors want to create a Blockchain-based Authentication System (BAS), that is designed to reduce the time and complexity of key distribution in platooning systems. BAS is a decentralized system, wherein each vehicle can derive a vehicle-specific key directly in the network. Therefore, when the platoon members share computational power, data can be processed securely. By skipping the use of a so-called trustworthy third party, like a Certificate Authority (CA), the risk of Single-Point-Of-Failure (SPOF) can be reduced. Multiple security issues addressed in this paper are applicable for V2X-communication and intelligent transportation system (ITS). There are different types of vehicles which have a platoon; all are interacting with each other and with the infrastructure. Since all the layers of the OSI-model are included, a lot of different security techniques must be made secure and scalable which makes it very complex and heavy.[8] To conclude, a blockchain-based authentication system for safe-assessment applications within a cluster of CAVs (CAV_N) is presented in this report. As the neural network is a machine learning model that can weigh fraudulent and good driving information, the Smart and Secure Vehicular Information

Exchange Algorithm (SSI) is designed to suppress malicious information sharing within clusters of connected vehicles, perform data filtration, and identify safe navigation mode within the cluster. On the basis of the authenticated safety assessment on the CAV network, a secure message format for safety assessment is designed to assess the safety of its network members. The Blockchain based Authentication System (BEST) will be able to improve CAV's safe-drive prediction ratio for an approximately twenty percent increase and an approximate twenty percent reduction in information accuracy due to network attacks rather than the common schemes for simulating friendly and related works.

7.2. Privacy-enhancing Techniques

Various blockchain solutions are proposed to enable secure access control in autonomous vehicles. They provide tamper-resistant registers for vehicle and IOT device data, prevent unauthorized access to the data and provide secure digital identities for participants. However, even with sophisticated access control architectures, situations may occur where security and privacy are compromised. In such scenarios, beneficial auxiliary techniques are privacy-enhancing techniques. Privacy-enhancing techniques in blockchain-based authentication for autonomous vehicles, it refers to a technical approach or cryptographic measure to protect privacy values. There are two broad categories of blockchain-based literature for privacy-enhancing techniques. One is about authentication of authorization and PPoP communication and the other is about privacy technique in a blockchain infrastructure by preserving identity anonymity [5]. The first category is the most solicited. It is based on the principle that a user's privacy can be protected by letting the blockchain prove possession of attributes instead of requiring to show them. In particular, a blockchain is usually used to guarantee the verifiability and transparency of the transaction. This aspect is usually referred to as privacy with authenticity. The concept includes, among others, confidentiality protection of the public values and privacy protection as well as of the users, which can be guaranteed through the privacy with authenticity. This broad concept recommends the use of privacy-preserving attribute credential and has been investigated in various autonomous vehicle scenarios such as focused on a privacy-enhancing attribute-based credential authentication with an anonymous revocation mechanism. Although indirect privacy is achieved, a blockchain is maintained to store necessary individual certificates. Another interesting technique is based on certificates encrypted by using the public keys of vehicles and sensitive data. This attribute-based scheme has the advantage of simpler proof generation. Moreover, achieving better energy consumption support is another challenge when dealing with multiple drivers in spawns of intersections. The performance comparison reflects that multi-TA-ABE outperforms the others in larger size and number of TAs, as well. Nevertheless, the performance test is not completely comparable as the proposed technique is directly, i.e., without blockchain support. Sometimes, a blockchain is also used to authenticate identity in autonomous vehicle setups. As one characteristic of requirements in security domains is that data is always confidential, it is the key factor for the success of a system to make sure that the confidentiality is intact. In another study, blockchain with complex attribute-based signatures was used and had superior performance than existing schemes. All the studies in the considered area answer the call to improve immediately the confidentiality and privacy of current systems. Input validation, nosiness, and unlocking of the car are highly relevant issues for autonomous vehicles. Some form of encryption and digital signature may be incorporated to solve the main security issues. A centralized and distributed approach has been proposed and showed its ability to improve confidentiality and privacy with respect to the centralized architectures. However, the challenges that the complete solution of privacy-preserving techniques and system integration needs are still under addressed.

8. Implementation and Deployment

It is obvious that as software entering everyday life, including vehicles, more stringent requirements will emerge and require additional consideration in their specification and development. This transition will require sophisticated new mechanisms for certifying the data collection, decision-making, and derived recommendations of these vehicles, without relying solely on vulnerabilities such as the immobilizer or key fob. On dynamic levels, as the capabilities of these vehicles become increasingly autonomous and their sensors become increasingly interconnected with one another, identifying physical control of a vehicle's operator (or lack thereof) will become increasingly complex. It seems that requisite cybersecurity measures may evolve indefinitely, leaving an autonomous vehicle or, worse, an inconsistent array of autonomous vehicles with a seemingly ever-growing range of behaviors and capabilities, as a relatively easy target for attackers [10] [1] [11].

Blockchain technology was initially developed for Bitcoin in 2008 and has since inspired a staggering array of business, societal, and governmental initiatives. Blockchain technology can not only bridge trust requirements for various use-cases of a solo domain but also assist trust requirements between multiple domains or parties. It provides capabilities like decentralization and immutability using cryptography, which validate the entire recording system's integrity. These capabilities benefit not only straightforward finance, but also extend across market verticals including autonomous vehicle systems, which are slowly gaining prominence.

8.1. Technical Requirements

The major aim of the role-based access control (RBAC) model in CAVs is to propose a procedure where effective communication across all communication mediums is possible without any security jeopardy. Thus, the user may have access to data and additional communication channels/ systems on the basis of the selected role in the vehicle. The proposed system can be further facilitated on blockchain technology in order to make it more secure and reliable, as it tallows access to authorized vehicles/ users only with non-repudiabillity and information integrity and confidentiality. [21] We are aiming to provide a decentralized, secure communication environment with access of data through selected authorized users with security. Thus, the role-based access control system proposed by us, covers maximum grounds without any security breach. The chapter proposes major components with the help of the latest technology of blockchain, in which, proper authentication can only take place by providing the necessary and appropriate authorization to the user selecting the role.

[22] The main aim of this chapter is to develop a role-based access control model using blockchain, a tamper-proof ledger, for efficient, decentralised, and secure access control in connected and autonomous vehicles (CAVs). The chapter earlier discussed the scope, challenges, and role of access control in CAV’s environment, which requires a high level of communication. This chapter has two major components. Access control module, in which access control decisions will be made, smart contracts for autonomous decisions, and a method for their integration in a CAV; and an access control management module for role-based centralized access control policy design and deployment.

8.2. Integration with Existing Infrastructure

[16]Blockchain-backed security strategies offer potential opportunities for improving driver assistance system security levels. By providing an additional security level to protect the

information stored in the system, as well as ensuring secure communication channels, modern cryptographic tools might contribute to dispelling the concerns of automakers regarding the tamperability of driver assistance systems. Although blockchain is advanced technology associated with concerns about low efficiency and scalability, it is widely used in critical sectors, including supply chain, healthcare, logistics, identity management, and financial services. The use of blockchain has not been verified in the automotive field for the privacy and efficient communications of autonomous vehicles.[7]The modern connected autonomous car can be seen as a type of mobile IoT device or, to some extent, a mobile server. All connected cars will become potential nodes in the IoT network and can communicate with other vehicles, roadside equipment, backend servers and also receive data from software over-the-air (SOTA) or firmware over-the-air (FOTA) updates. Therefore, the diversity of channel, the critical demand of safety and reliability, the demand of high-level security, the timely response of governmental regulation and the different policy of different vehicle makers give the automotive industry an urgent need to deploy identity authentication, access control, privacy protection and version management as a service or as a platform in the connected autonomous driving system. As driving performance depends increasingly on interaction among the intelligent connected vehicles, the infrastructure, the government and control centers, ensuring the integrity of chain of custody and providing trusted trip data for digital forensic data mining and data Al-driven processing attracts general consensus of the automotive industry.

9. Case Studies and Use Cases

The Internet of Vehicles (IoV) has received widespread attention from many researchers because IoV aims to improve the mobility, safety, and efficiency of roads. One of the challenges of IoV is security and privacy, which includes the issues of privacy and security of user data and vehicle data. In response to these problems, the combination of blockchain technology with IoV has become a research hotspot in the past two years. Furthermore, blockchain should reduce the real-time delay of on-chain transaction verification. Based on the perseverance of transaction verification results, it will be particularly important to improve the proposed solution and make it stable and efficient. [5] This chapter utilizes the Ethereum Ledger structure to propose a design, Secure Autonomy Environment (SAE), that harnesses V2X and blockchain technologies to conduct fast detection and security management, showing its advantages in traceable information management and control deployment. Simulation results demonstrate that the proposed schemes are cost-effective and robust against delay and node compromise attacks on edge computing utilization. However, the performance of our scheme is strongly influenced by the cost of writing operation in the underlying ledger and encourages the development of a light operation. Furthermore, solutions that optimize cryptographic operations are needed. No matter the effectiveness of blockchain technologies in autonomous driving, we need to identify the effectiveness of collaborative perception in different scenarios, and accurately measure the cost and latency of blockchain-based collaboration analysis.

[18] [23] This chapter provides the case studies and use cases of blockchain-based authentication systems in autonomous vehicles. Existing studies use blockchain in Vehicular ad hoc Networks (VANETs) to address problems such as key management, privacy, secure data transmission, and traffic safety. The cases have focused on three aspects: blockchain-based privacy protection authentication protocol for VANETs, consortium blockchain for data sharing among vehicles, and lightweight blockchain-based authentication for connected car networks.

9.1. Real-world Applications

[5] A privacy preservation scheme for vehicular ad hoc networks (VANETs). This scheme which the authors proposed called DiVaS, in which an anonymous vehicular infrastructure blockchain (AVIB) was proposed to generate secure and privacy-preserving certificates for the vehicles [10]. Additionally, a group signature technique was used to encrypt private data, and a secure and privacy-preserving public key encryption was used for public vehicle data to provide security and privacy-preserving mechanisms.[20] A blockchain-based privacy-preserving multiauthority scheme that aimed to share anonymized real location data. This scheme processes users' location data and extracts geohashes, which are then hashed and sent to an authority, after which an encryptions will be created. This scheme provides end-to-end privacy guarantees through blockchain and privacy-preserving spatial cloaking. A consortium blockchain, set with multiauthorities, was built to support the supervision and protection of the shared data. A batch authentication protocol for Internet of Things (IoT) devices that aimed to allow multiple IoT devices to perform the registration and authentication processes in a cooperative way. To register the devices, a double-authentication technique was used, where a registering device generated an authentication

official secret key which was shared with the nodes. To authenticate the devices, the user signature of new devices was generated and sent to the authentication server, which was then stored in the server's memory and the devices were added to the list. The Emergency data collection applications, traceability features, and colaborative security features applications.

9.2. Benefits and Challenges

To answer the question of whether newly developed architectures and algorithms for integrating direct connections between BBASs and intelligent vehicles are also protecting the privacy, a privacy and data security perspective needs to be included. Employing PSA, functional splits and the application of differential privacy (DP) can meet the absence of trusted third-parties within direct-connection-based BBASs. These would be operational for various intelligent vehicles and initiatives (where trust might not be always be present among vehicle entities). Researchers can add differential privacy to all incoming and outgoing data sets, which gets transferred between the BBASs and the ECUs of V2X equipped vehicles. Additionally, new queries can evaluate the change of the privacy and the correlation between the original and skewed data. The unique differentially private emulation algorithms can create the privacy-respecting queries that can be answered by the BBASs or returning privacy-respecting responses. Moreover, trusted and privacy-aware location-based services that are realized through previously developed location privacy respecting functionalities need to be added within BBASs [24].

Blockchain-based authentication systems (BBASs) offer numerous benefits for providing secure access control in intelligent transportation systems. Addressing direct connections between BBASs and intelligent vehicles, BBASs consider various needs and obstacles that are hindering the widespread adoption. Direct connections can perform keyless access control, can be used for fee-based value-added services and may also handle predictive maintenance and mobility services. The authors raise issues of uncertainty and privacy which is required for any BBAS implementation in the future. They propose a multi-layer BBAS which guarantees an optimal implementation of these important requirements and have created extensive plans for addressing these challenges. This article demonstrates that BBASs promise both exciting and challenging approaches for providing secure access control according to the range of vehicle types and various kinds of external entities. Furthermore, novel security, privacy and breaking-link countermeasures are presented and open issues are discussed that underline the implementations and usage of BBAS within a multi-layered architecture [23].

10. Future Directions and Research Opportunities

In the automotive supply chain management blockchain can secure the provenance and integrity of telemetric data linking them to vehicles and components in a secure, distributed and immutable record. This will help automotive suppliers to roll out the zero trust infrastructure to en- able trust and operational integrity between components/nodes. Representative examples include a solution securing telemetric data and event planning inside electronic control units and a blockchain agnostic solution to track the data flow across the lowest stack of the vehicle's architecture [1].

The other research opportunity is leveraging blockchain-based trust among electrics control units for secure vehicle communication and operation at a micro-scale. This will allow direct interaction between electric control units based on the consensus of their verifications combined with consensus within a blockchain, thus bypassing any centralized trust authority [22]. The current security topologies in connected vehicles are challenged by large scale component interactions, delayed imbalance acknowledgement for service load management, regulatory compliance with automotive industries, lack of solid solutions for lower tier supplier involvement, and undefined software/hardware security personality among TierXed suppliers.

Blockchain has a bright future in the fields of autonomous vehicle security and automotive supply chain management. For autonomous vehicle security, blockchainbased solutions are optimized for V2G, V2I, V2V communication, and backend autonomous vehicle systems and offer integrity, transparency, accountability to minimize various identified threats. In addition, blockchain-based conditional access can disrupt traditional certificate-based security architectures and protect data privacy during communication with Verifiers [10].

10.1. Emerging Trends

The rising trend of connected vehicular communications is the potential applications of Blockchain to locking mechanism issues. Various researchers have recommended numerous blockchain-oriented research frameworks and platforms for emerging technological improvements in vehicular atmospheres, among which permissioned Blockchains and hyper ledger-based consensus algorithms seem to emerge as leading contenders. Vehicle to vehicle and vehicle to infrastructure communication is the crux of Connected Vehicle Systems, which presents multiple security related issues to be solved, with privacy preservation at the top. They develop a hyper ledger block chain-based access control platform that involves all neighbouring vehicles of a specific vehicle and use Smart Contracts to form a collective access control management policy among them. Blockchain consortiums gain prominence over permissioned Blockchain when supporting a large set of access control, consisting of ongoing and resolved access control manifests, from those trustable administrators who directly or indirectly administer a plethora of exposed vehicles and service beacons. Therefore, this work has the potential of being generalized to encompass many trustful organizations to form a trusted, distributed V2X network operating environment for seamless deployment.

[6] [22]Authentication and access control is essential for secure communication in the environment of connected vehicles. Researchers are utilizing Blockchain in addressing authentication and access control challenges in cybersecurity, specifically in the realms of IoT and IoV. Blockchain as a technology can cater for decentralized credential management and dispense confidential user information, risks mitigating the issues of single-point-of-failure and high exposure to the man-in-the-middle attack. For addressing security concerns in connected vehicles, chiefly two methods are popularly embraced Single Sign-On (SSO) and Multi-Factor Authentication (MFA). The Blockchain-empowered system Mrs. John uses a cryptographic primitive to provide a secure establishment and verification of network entities. The proposed model is to be harnessed to provide secure communication within IoV for autonomous vehicles.

10.2. Potential Enhancements

Several significant enhancements can be made to the current cryptocurrency and blockchain techniques for even higher security. A decentralized Partial Trust Authentication System (PTAS), as well as a Blockchain-based Fully Decentralized Vehicular Public Key Infrastructure (VD-PKI) can serve typically by enhancing Ethereum to be used as a more trustable and efficient validator in plasma. Blockchain allows a way of making asynchronous draws on funds while ensuring that non-cooperating parties will not block the draw. Using models and formal proofs, it is shown that our notion of forking underlined by a recent formal definition of safety satisfies our requirements fully, resulting in a directional blockchains extending sequence <B0,. . ., Bn> from Genesis block to Bn, extended in the healthy portion B0,. . .,Bm whichever, m < n, but rejected and declared safe directed by a pre-defined inclusive-prefix of the m chain's prefix faces validation stamp.

[2], [25]

11. Conclusion and Summary

Integrated functions among 'IoV/AV cloud VTTLI service', 'IoV/AV cloud VDTF service ' and 'IoV/AV cloud TDUSB' are supported by the proposed architectural model, which not only can provide secure access and synchronous location of the various information service peripherals from the AV, but also allow the authorized smart phone and the IoV-NCA interact through the IoV-NC for mutual diagnosis or service provision [6]. Because blockchain service providers can authenticate sources of IoV-NCA for the security of blocked IoV-NCA can be ensured, and the primary advantage of using blockchain of trustability, tamper-proof and traceability. Furthermore, the execution time and computational power of the proposed authentication and access control design and various communication processes are relatively efficient in the computational performance evaluation.

Autonomous vehicles (AVs) are the main trend of transportation vehicles, which have begun to gradually percolate from the concept stage to real applications in industrial production and people's lives [12]. In the future, AVs may communicate with a variety of service peripherals in the Internet of Vehicles (IoV), and the authentication and access control within the IoV are significant issues for the safety and health of the passengers as well as the AVs themselves. This paper presents in detail the densely and sequentially distributed architecture of heterogeneous authentication system of IoV for AV (HASIA- IoV-AV) including Vehicle Autonomous Identity Authentication (VAIA) module, Intelligent Transport System (ITS) provider Intelligent Vehicle Cloud Services Platform (IVCSP) and common IoV after SALSM. We also summarizes the salient security features of IVCSP based on the blockchain technique.

11.1. Key Findings and Contributions

[6] [18] [2]The key findings and contributions of this chapter are summarized as follows: • We have extended the existing single sign-on (SSO) mechanisms into semi-decentralized SSO where different use cases of SSO are implemented using Ethereum smart contracts. The proposed mechanism contributes in the development of real-time inter-vehicular services.

Our millage-based fuel control system has potential to be used in current vehicular services infrastructures and can lead to mass use case as soon as it is commercially available. • Our proposed MFA access control system utilizing blockchain contributes strongly to recent discussions on the security of ISD systems in the V 2X context. The proposed MFA solution would be relevant for applications in the service-based communication paradigm being defined in the V 2 X communication in the future of mobility. Because the recent development is the service-oriented architecture (SOA) paradigm, the presented solutions will be useful in the near future. • Our sensors can utilize the Ethereum blockchain for certification, and implement security communication based on secure multipart computation methods. Our two-factor certified temperature alarm system thus provides not only flexibility in means of communication and protection of constant confidentiality of reference values, but even preserves data integrity among different stakeholders (towmillage, confectionery, etc.) without the need for the stakeholders to trust a third party (Dachi et al. 2019).

11.2. Final Remarks

The intuitive success of public chains and their potential for the IoV can make the already well designed PoS coin implemented in a vanet a substantial technological head start and a more consolidated model for the open ecosystem that the unrestrained communication between vehicles belongs to.

In this way of interaction with a blockchain network, the preventive protection needs can be better satisfied than in the case of defining security measures assuming a special entity requiring protection (client, server, etc.). The tailored structures can be used among other for minimizing the inter-operation expenses caused by mismatch between functionalities of underlying components, deep customization of communication protocols or deficient link adaptation mechanisms.

Even earlier, a backbone structure of a blockchain system with PoS based consensus was discussed for vanets in [7]. PoS is considered a lightweight protocol in comparison to PoW (i.e. implemented in Bitcoin). Moreover, a deterministic concept of establishing the blockchain infrastructure was proposed.

The papers [10] and [20] also had this concern and focused the article on security in vehicular networks, exploring the blockchain-based authentication. We believe that our survey also brings a contribution towards this paradigm.

References:

1. Vemoori, Vamsi. "Envisioning a Seamless Multi-Modal Transportation Network: A Framework for Connected Intelligence, Real-Time Data Exchange, and Adaptive Cybersecurity in Autonomous Vehicle Ecosystems." *Australian Journal of Machine Learning Research & Applications* 4.1 (2024): 98-131.
2. Sadhu, Ashok Kumar Reddy, et al. "Enhancing Customer Service Automation and User Satisfaction: An Exploration of AI-powered Chatbot Implementation within Customer Relationship Management Systems." *Journal of Computational Intelligence and Robotics* 4.1 (2024): 103-123.
3. Tatineni, Sumanth. "Applying DevOps Practices for Quality and Reliability Improvement in Cloud-Based Systems." *Technix international journal for engineering research (TIJER)*10.11 (2023): 374-380.
4. Perumalsamy, Jegatheeswari, Chandrashekar Althati, and Lavanya Shanmugam. "Advanced AI and Machine Learning Techniques for Predictive Analytics in Annuity Products: Enhancing Risk Assessment and Pricing Accuracy." *Journal of Artificial Intelligence Research* 2.2 (2022): 51-82.
5. Venkatasubbu, Selvakumar, Jegatheeswari Perumalsamy, and Subhan Baba Mohammed. "Machine Learning Models for Life Insurance Risk Assessment: Techniques, Applications, and Case Studies." *Journal of Artificial Intelligence Research and Applications* 3.2 (2023): 423-449.
6. Mohammed, Subhan Baba, Bhavani Krothapalli, and Chandrashekar Althat. "Advanced Techniques for Storage Optimization in Resource-Constrained Systems Using AI and Machine Learning." *Journal of Science & Technology* 4.1 (2023): 89-125.
7. Krothapalli, Bhavani, Lavanya Shanmugam, and Subhan Baba Mohammed. "Machine Learning Algorithms for Efficient Storage Management in Resource-Limited Systems: Techniques and Applications." *Journal of Artificial Intelligence Research and Applications* 3.1 (2023): 406-442.

8. Devan, Munivel, Chandrashekar Althati, and Jegatheeswari Perumalsamy. "Real-Time Data Analytics for Fraud Detection in Investment Banking Using AI and Machine Learning: Techniques and Case Studies." *Cybersecurity and Network Defense Research* 3.1 (2023): 25-56.
9. Althati, Chandrashekar, Jegatheeswari Perumalsamy, and Bhargav Kumar Konidena. "Enhancing Life Insurance Risk Models with AI: Predictive Analytics, Data Integration, and Real-World Applications." *Journal of Artificial Intelligence Research and Applications* 3.2 (2023): 448-486.
10. Pelluru, Karthik. "Advancing Software Development in 2023: The Convergence of MLOps and DevOps." *Advances in Computer Sciences* 6.1 (2023): 1-14.
11. Selvaraj, Amsa, Bhavani Krothapalli, and Lavanya Shanmugam. "AI and Machine Learning Techniques for Automated Test Data Generation in FinTech: Enhancing Accuracy and Efficiency." *Journal of Artificial Intelligence Research and Applications* 4.1 (2024): 329-363.
12. Konidena, Bhargav Kumar, Jesu Narkarunai Arasu Malaiyappan, and Anish Tadimarri. "Ethical Considerations in the Development and Deployment of AI Systems." *European Journal of Technology* 8.2 (2024): 41-53.
13. Devan, Munivel, et al. "AI-driven Solutions for Cloud Compliance Challenges." *AIJMR-Advanced International Journal of Multidisciplinary Research* 2.2 (2024).
14. Katari, Monish, Gowrisankar Krishnamoorthy, and Jawaharbabu Jeyaraman. "Novel Materials and Processes for Miniaturization in Semiconductor Packaging." *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023* 2.1 (2024): 251-271.
15. Tatineni, Sumanth, and Naga Vikas Chakilam. "Integrating Artificial Intelligence with DevOps for Intelligent Infrastructure Management: Optimizing Resource Allocation and Performance in Cloud-Native Applications." *Journal of Bioinformatics and Artificial Intelligence* 4.1 (2024): 109-142.
16. Sistla, Sai Mani Krishna, and Bhargav Kumar Konidena. "IoT-Edge Healthcare Solutions Empowered by Machine Learning." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.2 (2023): 126-135.
17. Makka, Arpan Khoresh Amit. “Integrating SAP Basis and Security: Enhancing Data Privacy and Communications Network Security”. Asian Journal of Multidisciplinary

Research & Review, vol. 1, no. 2, Nov. 2020, pp. 131-69, https://ajmrr.org/journal/article/view/187.

18. Katari, Monish, Lavanya Shanmugam, and Jesu Narkarunai Arasu Malaiyappan. "Integration of AI and Machine Learning in Semiconductor Manufacturing for Defect Detection and Yield Improvement." *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023* 3.1 (2024): 418-431.
19. Tembhekar, Prachi, Munivel Devan, and Jawaharbabu Jeyaraman. "Role of GenAI in Automated Code Generation within DevOps Practices: Explore how Generative AI." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.2 (2023): 500-512.
20. Peddisetty, Namratha, and Amith Kumar Reddy. "Leveraging Artificial Intelligence for Predictive Change Management in Information Systems Projects." *Distributed Learning and Broad Applications in Scientific Research* 10 (2024): 88-94.
21. Venkataramanan, Srinivasan, et al. "Leveraging Artificial Intelligence for Enhanced Sales Forecasting Accuracy: A Review of AI-Driven Techniques and Practical Applications in Customer Relationship Management Systems." *Australian Journal of Machine Learning Research & Applications* 4.1 (2024): 267-287.