Human-Centric Authentication Systems for Secure Access Control in IoT-connected Autonomous Vehicles

By Dr. Mads Nielsen

Professor of Computer Science, University of Copenhagen, Denmark

1. Introduction

User convenience, efficiency, and security must be kept in mind when proposing any new mechanism for authentication [1]. In the IoT-connected AV ecosystem, users interact with the in-vehicular infotainment and entertainment system (IETS), vehicle control system (VCS), and autonomous vehicle service control system (AVCS). These systems are composed of a variety of applications, including media players, voice assistant systems (VAS), internet browsing, in-vehicle vehicle-to-vehicle and vehicle-to-infrastructure (V2X) communication, GPS navigation, and various types of sensors. All the applications are operated via different input/output (I/O) modules, including touch screens, voice sensors, and smart wearable devices. Hence, we have proposed human-centric secure identification and access control for the involved IoT applications in different subsystems. Furthermore, we have proposed a system that can support distributed and edge computing environments as well as the cloud access control server.

As per the recent International Data Corporation (IDC) report, the total size of the global datasphere was forecasted to reach 175 ZB by 2025, and the number of IoT connected devices was expected to reach a staggering 41.6 billion by 2025, generating 79 ZB of data annually [2]. One of the biggest contributors to this surge in the number of connected devices will be the automotive industry, which is expected to play a significant role in the growth of the Internet of Things (IoT) and cyber-physical systems (CPS) [3]. These advancements would pave the way for a new paradigm of mobility services driven by autonomous connected vehicles by the end of 2020. Autonomous vehicles (AVs), enabled using the ecosystem of IoT devices, will become an indispensable part of future smart and connected urban- and rural-societies, communities, and environments. With the proliferation of IoT in every society domain, securing data transport between IoT sensors from vehicles to servers and clients will be

essential. This paper is therefore focused on developing user privacy- and authentication-aware access control mechanisms for the IoT-empowered autonomous vehicles.

1.1. Background and Motivation

Authentication systems like facial-recognition-based systems have several challenges. For example, rule-based systems cannot perfectly work for different conditions, and other biometrical features, such as facial masks, hairstyle, or makeup, may affect the decision in a negative way. It is also possible to have false decisions when people keep their heads in a slanted position. Therefore, head, face, and shoulder parts are important to be visualized in these systems to reduce these kinds of issues. Privacy and security problems can occur in human-centric systems, but researchers still are trying to overcome them to obtain new human-centric authentication approaches. Most security authentication research papers work on neural network-based recognition methods or deep-learning-based solutions [4]. Neural-network-based recognition methods provide high accuracy on reliable features; for example, deep learning can work well to avoid face-based recognition problems, such as variations in face appearance. In safety-critical systems like IoT-connected autonomous vehicles, human-centric authentication techniques can be effective if they are applied together with multifactor and multiview fusion for proper security and reliability.

Security is a major concern in IoT (Internet of Things)–connected autonomous vehicles. Unprotected connections between cars and IoT systems or people and IoT devices can lead to security threats or even car hacking. To address these, trustworthy and secure human-centric authentication systems should be developed for secure access control in an environment connected by IoT systems. In order to be trustworthy and secure, an authentication system should be capable of identifying an individual using many different unique identification factors, and prove the identity of the person in a non-forgeable way by making use of all these factors [5]. Human-centric authentication systems based on digital representations of facial, fingerprint, palmprint, or voice modalities are different gait models. They can be used in parallel or in a combined way to obtain a higher security level. The templates extracted from these modalities are matched with their templates from the database to authenticate their identities.

1.2. Research Objectives

The second original contribution of this paper consists of the prototype implementation of the A-IoT-HCA multi-modal authentication system through the Autonomous Car Control and Monitoring (ACCM) application. The second research objective set is to define the user authentication method that is going to involve both the lab analysis of the user behavioral patterns and the quasi passive liveness state management [ref: article_id=cf2ae8b6-65de-4f73-970c-026c35ac8e16]. In particular, the traditional car keys are the ordinary example of quasi passive protection. A valid alternative for the A-IoT-connected cars world could replace the car key with the combination of the proposed user authentication, which we argue to be more secure as well as easier at the same time. Such an innovative approach for adaptive user authentication when used with IoT-connected automobile system enables a successful return in practical guaranteeing secure and correct car control just by the driver's behavior.

The research proposed in this paper focuses on integrating an HCA approach into an IoT-connected autonomous vehicle for mitigating the undesired consequences of potential maliciousness or failure attacks, where human actions are used as secure input in the process of user authentication and access control. The first original contribution of this paper is defining the theoretical HCA three-layer model that allows analyzing the behavior of each HCA layer for assessing A-IoT's security weaknesses before signaling a decision to invoke a plausible A-IoT application attack. The aim of the first research objective set in Section 1.2 is specifically defining the resources, such as data sources and levels of computational complexity, to be used by each of the three HCA layers [ref: article_id=22b454a3-54e0-48b6-8928-844b9bdaa4c9]

1.3. Scope and Limitations

Peer-reviewed security mechanisms and protocols in the form of authentication, identity management, access control etc., founded significant contributions from a larger pool of researchers. In the context of IoT-connected autonomous vehicles, the emergent frontiers around the literature review premises the heavy influence on visible light communication and window-to-vehicle communication bearing full compatibility with up-and-coming smartphones or other hand-held consumer devices. Therefore, such solutions are generally restricted to the conventional F2G deployments. However, from the standpoint of vehicular communications, albeit mmWave evinced to exceptional compatibility with prospective

automotive services, yet it is over looked in this research to avoid its issues related to scalability and compatibility.

With rapid technological advancements, the trend of autonomous vehicles is emerging, and it is anticipated that by 2050 all new vehicles will be autonomous electric vehicles [1]. The aforementioned scenario is coined smart mobility or simply smart transportation. The facets of autonomous vehicles encompass multiple usage scenario such as having connected entities with/without human intervention viz., IoT entities [6]. The human-centric perspectives in the autonomous vehicle system largely concentrate on smooth and ease of communication with this system, secure user and vehicle privacy etc., [7].

2. IoT-connected Autonomous Vehicles: Overview

IoT as an open platform for numerous applications becomes the hub of security and privacy threats caused by malware, attack surfaces, network attacks and communication attacks like plagiarism, falsification, privacy disclosures, anonymity revocations, impersonations, betrayal, frames, message playing, and selfish behavior. In this direction, security and privacy proofs using a validated and secure authentication system. However, attacks and the number of authenticated entities, subsequentity, manual registration and authentication management, real privacy, real attribute dynamics, real-time performance are still open problems in a given IoV scenario. The traditional computer resources are secured and authenticated based on cryptographic security plots. In case of traditional cryptographic parameters, resources have significant computational costs according to their ability to perform highly secure and authenticated cryptosystems. The ability of IoT/ IoV enabled cryptosystems are not only defined by their computing capabilities to authenticate and secure the resources but also low power, economic and real-time demands under the IoV. Thus, IoT/ IoV resources and cryptographic security mechanism lead to considerable, and it is challenging to incorporate them with the major open parameters. Open authentication, encrypted thoughts and management of IoV based cryptosystems based on devices and sharing data from the IoT AP on the IoV edge. It is the aim of the article to shed some light on the future trends of privacy and security in vehicular edge computing and IoV to enable holistic strategies and measures for the development and smooth advancement of these technologies. Moreover, we also emphasized specific IoV Simulation based Tools that provide solutions to these challenges and future trends that enable the latest IoT-based technological era to be fully automated. [8]

A revolution is underway with the integration of the Internet of Things (IoT) and artificial intelligence (AI) to create interdisciplinary and connected world—smart world. Classically, with Machine to Machine (M2M) communications mechanism, the IoT promises to connect things. Here, things exist in the form of objects, smart devices, sensors, vehicles, buildings, household and many more. In recent years IoT-enabled autonomous vehicles (IoV) have gained international momentum as a new evolution in the automobile industry. Autonomous vehicles (AVs) also called self-driving cars and driverless cars are capable of performing tasks without human physical presence. Sensor-rich IoT-empowered AVs are getting more attention as independent IoT objects. The continuous data gathering makes them a unique data source and problem solving technique. They continuously sense, communicate and collaborate to transform as a source of perception, prediction, and actions. Its collaborative intelligence (Or IoT in the road) can assist in many issues such as traffic managements, public safety, reduce congestion, reliable driving, Weather-aware drive, energy conservation, Entertainment, reduce emissions and improve passengers comfort. This potential amassed pathways toward IoT-empowered autonomous vehicle technology. Indeed, the road to the autonomous cars on the IoT communication lane has been constructed and becoming a reality. However, security, privacy, and trust are inherently inherent in the integration of IoV and IoT, as per the hybrid environment created and the various glioma exposed to cyber-attack. Security ensures that the system operates under the specified circumstances without negative effect. Privacy is about data and the control of the data and its visibility, whereas trust is a belief in the reliability and ability to perform a specific task securely.

2.1. Key Components and Technologies

[9] Smart sensing mechanisms can, for example, detect unconscious or incapacitated passengers to automatically take corrective and preventive mechanisms. Other applications may include protecting passengers during threats or emergencies. Identity authentication systems are foundational to secure IoT-coupled smart sensing mechanisms using connections between different entities including a vehicle and devices and servers. The most common authentication scenario involves an authentication protocol performing the verification of a user without activating complex algorithms or processes, most often taking refuge in compromised credentials to authenticate. Biometric-based mechanisms are also integrated with existing systems to ensure a user is authenticated biometrically which are vulnerable to specific attacks.[3] Surveys show that there is no centralized authority or standard in the IoT,

making it one of the most challenging research areas in security and privacy fields. Due to an increasing interconnectedness of entities and the natural vulnerabilities of IoT systems, security and privacy issues will remain among the most challenging from a research perspective. The main factors that security in the IoT should consider protecting are the source integrity of transmitted information, confidentiality, authentication, and the non-repudiation of information. Securing IoT devices' identity is key and serves as a first step before any other services are offered. Additionally, to secure the IoT, three main points need to be considered: secure communication and transfer of data, secure authentication of different devices, and secure management of devices such that a hacker cannot get control over a device.

2.2. Challenges and Security Concerns

Our work complements this previous study by focusing mainly on the verification and authentication of users of these devices which should be as efficient and secure as possible to mitigate security threats in IoT devices [10]. To implement authentication efficiently on IoT devices a few categories of research are being conducted. Some recent studies suggested that different methods can be used for IoT device authentication. For example, Bansal et al. suggested the elliptic cryptography-based authentication method which can reduce the security overhead requirement, therefore, it can support the limited legacy devices [7]. MacEwan argued the need for a more efficient authentication mechanism for IoT devices. Public key cryptographybased authentication generates a large computational overhead and thus is unsuitable for IoT devices due to the requirement for high computing power. The use of blockchain-based methods for IoT device authentication could be a potential solution to this impediment. Blockchain technology is emerging as an alternative for secure, reliable, and transparent communication systems. Blockchain has gained attention in several domains, including cryptocurrency, decentralized networks, consent management, smart contracts, and distributed trust. Blockchain is emerging as a promising technology for the secure management and communication of IoT devices and support seamless, transparent, and reliable operation [3].

Smart homes equipped with various devices connected via the Internet of Things (IoT) has become an essential part of domestic life. Moreover, with the advent of autonomous cars, vehicles are increasingly connected with the IoT. As a result, vehicle-to-vehicle and vehicle-to-infrastructure communications are contributing extensively to the Internet of Vehicles (IoV

or sometimes called VANETs, Vehicular Adhoc NEtworks). In IoV, vehicles and infrastructure nodes are connected via the IoT, and they interact via IoT networks to provide many services, including safety services, mobility services, and environment protection services. In general, the vehicular network environment requires different mechanisms to ensure secure communications and to provide secure services. Some of the security measures commonly required for IoV are providing data integrity, geographical messaging, prevention of impersonation attacks, black-hole attack detection and prevention, data privacy, secure authentication, and authorizing communications before starting it. These security measures are usually achieved using different cryptographic algorithms for vehicles and infrastructure node communications and for vehicle-to-vehicle communications. They also involve using cryptographic technologies with digital certificates or group signatures to support secure IoV communications.

3. Authentication Systems in IoT-connected Environments

Multi-factor authentication (MFA) enables users to more efficiently prove their identification to the system by presenting two or several various personality proofs. There is a compendium of ways of proving the MFA, which are generally grouped into "Factors". Like something only the user has got, like a security token or mobile phone, is something that represents this factor. Something only the user identifies, such as a password or personal identification numbers, comes in the category of Something that the user knows. Biometric identification procedures determining which an entity is, such as behavioral or physiological properties, make up the final category of MFA. Biometric specifications are allocated as the strongest classifiers in MFA approaches. However, the extent of trust in biometric-based systems is mostly tied to its privacy and security considerations. Moreover, the requirement for the user to associate with the feature, however small, makes the centrally presented biometric system vulnerable. Security-conscious corporations, as well as the academic and privacy-wise, mostly debate biometric and centrally presented services and the allocation of the truth. They still see the biometric aspect of user personality and hence see the dangers of misreporting, enhancing the danger of identity theft in MFA procedures [4].

Authentication is a process within cybersecurity and privacy that verifies the reliability of users via their identities before they gain access to systems, which in turn helps these systems ensure protection against unauthorized access. In the traditional system the authentication

process occurs at the periphery of the network and uses a variety of user-specific conditions such as username/password. In the course of the past two decades, authentication mechanisms have evolved to meet the requirements of connected-device ecosystems. Decentralized authentication will be an essential building block for digital identities in the IoT [1]. The number of connected devices will lead to an expanded usage of decentralized identity systems in a variety of IoT ecosystems. When employing the decentralized identity concept, devices will possess an identity rooted in the interoperable nature of a decentralized identifier. They can substantiate claims in the form of verifiable credentials to interact with any IoT system. Blockchain technology plays a critical role in realizing decentralized identity in an ecosystem and is used as an unchanging and immutable registry. This approach is in contrast to the traditional root certificate-based mechanism in IoT identity management. When involving decentralized identifiers within IoT, the accountability roles besides the devices, namely, the owner, reseller, user designer, and verifier, have to undergo reconsideration in IoT chain-of-trust environments. They come with their own roles, relationships, ownership, policies, and verification tasks in the DPIoT environment [11].

3.1. Traditional Authentication Methods

In the scenarios like the efficient authorization identifications for actual IoT device clients and backend server and request/querier authentication transactions in the process of service chain invocation and request/querier chain amusement, IoT device clients can progressively repair and reset batch identities and arrange access passes to arrive to backend servers if original ones are found vulnerable to be lost easily [10]. It is lately claimed in this thesis that the unknown Bitcoin Elliptic Curve Parameter Elliptic Curve identity setted in the physical secure zone of the advanced bitcoin wallet certificatory Bitcoin elliptic curve base architecture of the smart phone or online service center has been exploited to extend a secure network adaptive bitcoin elliptic curve identity set for the smart phone and online service center accordingly. In the friendly interactive setting of an advanced Bitcoin blockchain wallet card, the BTC raised might already have been deposited by the original hardware vendor to the corresponding blockchainaddress-wallet.

The public key-based authentication (RSA and ECIES) and public key infrastructure (PKI) schemes are the most traditional methods in data transmission control and public key distribution in modern computer networks [12]. These classical cryptographic schemes have

been practically deployed for various network security applications, and the performance of these schemes are considerable acceptable in some cases. Then, the Authentication and Key Distribution based on Public Key (AKA_P) scheme is chosen specifically structured one-time passwords (S3DA) to authenticate users and establish a session key in the 4G mobile network. Fault-isolation in the S3DA protocol has also been studied as this work has recently been joined with sophisticated elliptic curve techniques for a new kind of cryptographic key exchange version. Before deployment to the 5G network, as an application at the middleware, service-layer and system-level in the end-to-end service chain of the Internet of Things, the extracted system architecture of elliptic curve outside authentication and keying service through intelligent devices has also been kludges to the 5G IoT. The strong RSA and ECIES asymmetric password correlation function is also scheduled to serve as an unknown customizable mining function instead of the cryptographic hash in the BTC ecosystem [13].

3.2. Biometric Authentication

Voice biometrics can be authenticated / verified in the customer service sector, and hearing and speech can be conducted in character recognition and agricultural studies. Windaws Hello is one of the applications that use support to enable authentication via Windows devices. Signatures can be trained with real signatures in file systems and can be used to perform real signatures. In, the author compares popular biometric sensors with a comparative study of their advantages and disadvantages in detail, while also taking into account the results of biometric facial framework in detail. Eyes and faces and face details are the most important biometrics because of the ease of execution of the autonomous authorization process [14]. Systems use different sensors to retain face and iris information of the objective container. Your iris is unique and does not change during your lifetime thanks to seven indicators, different photos, or your approximate images.

Biometric authentication could include DNA, fingerprint and iris recognition, electrocardiogram (ECG) signals, hand geometry and gesture scans, voice authentication, gait recognition, thermal authentication, vein authentication, face and face detection, facial expressions, eyebrow movements, mouth movements, lip, lip print, mouth shape, lip biometrics, ear and ear recognition. Among these categories, the use of biological patterns such as voice, face, palm print and signature for personal identification, keyless smart home entry and online privacy are gaining in popularity. Morever, Keystroke dynamics (KD), which

is based on the latency of typing, are also used for accent authentication. Biougraphy adds a dynamic side to the writing mechanism and the content of the letter compared to the formal biometric feature of the signature.

3.3. Behavioral Authentication

[15] [3]When it comes to IoT-connected AVs also it has to be kept in mind that an extra layer is added to it in terms of human interaction. The human along with vehicle-company has its own share of rights and responsibilities, thus there should be a suitable bond formed between the human user and his vehicle especially when it comes to access privileges of vehicle functions and furnished data. The digital identity of the physical driver will be the bonding factor between the two entities. Most of the vehicular AD applications cause for a driver in the loop and thus behavioral factors of human beings come in to pictures too. The behavioral traits (such as keystroke dynamics, touch dynamics, finger movement during touch are well recogni-zed behavioral biometrics) provide a platform where the users can be monitored passively for an improved monitoring and led to advanced functionalities. The radio signals extracted from neighboring mobiles can also be utilized for the same purpose however, it is always ideal to shrink data transmissibility as much as possible where the channel space is limited and very crucial. Also, it is preferred to not to involve any modification in the vehicles own E-Net due to it can tell adverse affects on its reliability to accept network. Consequently, we always prefer to have unmodifiable solution into consideration. The very form of passive monitoring named above is currently under exploration to apply the concept of IoV. According to the contact behavior feature of a physical user (normal mode of usage, hard-touch mode of usage, and fast responses), many diversities exist and are difficult to mask with the intelligence of computers and owners' usage habits . On the other hand, if the driver can touch a region of the display module with normal speed, it will be identified as "A", with fast touch speed as "C", and with a hard-touch speed as "B". In the evolution phase of the interaction between AVs and human use, due to various adverse factors, we cannot afford to risk the traditional RSA keys and ECDSA certificates. For examination of vehicles on Indian roads as of 2019 itself, only M2 and N1 category vehicles are allowed to test to perform level DVs experiments. In some sense, even the American American Association of Motor Vehicles predicted, all other types of level one each. It is desired to sudden starting of level three for many decades as such new brands onnest models and different level of users compatibility and acceptance testing and punishing will take long time, thus now we need maximum efforts

on approach of handling level D and E DVs as of today for the safety and security if the country eyes to establish the technical leadership of the globe. Even of the country is yet to introduce the concept of AV-software-testing-inspection-approval processes software, from scratch, no one existing levels and new concepts shall be considered.

4. Human-Centric Design Principles

Leveraging wearable sensor devices for continuous authentication holds the potential to fill this widening gap in the protection of human-centric and sensors-plus-facts systems. A user may never be bothered in any way about passwords, yet still be logged on and receive system services. The continuous authentication process may analyze sensory data to decide, fitting to systems, for residuals of probability density mass that build up within the perimeter of the cumulative distribution with strong edges around the cascade under construction to reject latecoming samples of the cascade as appearing malicious. Not being late enough on the other hand statistics in the time domain protest to be fully legitimate authenticated users. In the conclusion we note that the principal data structures, when representing pieces of real numbers, and the devices that enable provisionally contemplating them, have never in the past appeared in the crowd of secure multi-data transactions, but have the potential to stay there for a very long time now as they are useful, enjoyable, wearable in creatures of nature's make and they advertise the time incessantly [5].

Existing wearables have already been adapted for continuous user authentication in relation to specific applications. Existing methods may be repurposed, or new sensors and analytical tools can be wrapped into pendants, wrist wearables, rings, belts, clothes, shoes, headgear, or similar articles with fashionable but inconspicuous urban design. These wearables may have special functions like sizes, orientations, textures and so on. Other wearables may provide amusement, such as with games and performance art. But in contrast with these established paradigms, our approach emphasizes the topic of enjoying sensual data transactions directly by feeling in the most native, natural way necessary probability densities emerging from directly observing sensor data [16]. The user is never forced to take notice of any segment of data by increasing or decreasing the size of graphs of the variable involved, but obtains possession of data slowly with a pace that encourages a duty to exercise curiosity, and with an increased presence-to-data-density-ratio that is felt as being enjoyable and stimulating.

4.1. Usability and User Experience

[17] [18] In autonomous transportation, user information is required for both trip completion and mission actuation, and user information is made more salient as the car can intervene during autonomy execution and request interaction with users. Thus, the transformation to human-centric security and privacy is particularly urgent in the automotive industry, where existing conformal cyber security and privacy verification methods are not equipped to address the security and privacy needs of the human-centred systems in which the human is a key stakeholder. Existing auto-ID verification concepts in the automotive industry centre around the vehicle as the sole entity whose identification is verified. This class of ID verification includes vehicle-run ID verification and vehicle-to-external device ID verification; both of these classes centre on a physical device—the car.[5] When considering security from the perspective of the arrival of cars that are always connected to the internet and driving autonomously, the human emerges as the most important entity for determining the safety and security of the car, and it becomes especially important to verify the identification of the person. Thus, with cyber security and privacy as key concerns, it will also be the case moving forward that, as security and privacy threats in autonomous businesses spread more broadly and become more diverse, security technology will not be able to properly secure vehicles without having achieved a deep understanding of the human.

4.2. Privacy and Trust

Another key challenge to address in implementing human-centric authentication systems is to establish trust between passengers and the technological credentials. This is important, as system that are not trusted will not be used. User trust and adoption of autonomous vehicle technology are subject to the user's psychological, emotional and cognitive experiences. The emerging trust in automation from the communication of user experiences under adversarial conditions needs to be understood to ensure a smooth transition from research to commercialized autonomous vehicles. Comprehensive system testing, including stress testing, to understand trainees' cybersecurity maturity and trust adaptation in autonomous vehicle cybersecurity incidents is required to make guidance on privacy, cybersecurity, and ethics in driver-and passenger-based human-centric authentication. Accurate communication of potential future adversarial conditions can provide users with cues to respond appropriately. We conducted a survey to assess passenger anxiety while using the proposed systems that includes all adversarial conditions that the authors could think of, including adverse weather conditions. Twenty-three per cent of the intelligent Platoon participants,

fifty-nine per cent of SIoV participants and seventy-six per cent of SoV participants reported that they are sometimes anxious while a cyber-attack is exerted. We are currently conducting studies to assess whether passengers are anxious when system security is compromised [19].

We have proposed a user-centric system that is invariant to adversarial behavior by applying blockchain-based data interchangeability. Critical information needed by the vehicle is transformed into data with similar statistical characteristics as the original data. Therefore, adversarial behavior and data leak compromise the efficacy of misleading the attacker while protecting individual privacy. We have also introduced the concept of self-sovereign identity (SSI), which gives passengers the choice if they want to be anonymous. Such systems eliminate the need for user interaction and provide significant improvements to runtime performance while achieving similar levels of security. However, improving user trust should be a cross-disciplinary approach. Our proposed privacy-preserving SSI system gives passengers the choice if they want to be anonymous, i, the system is designed to support the privacy of passengers as our primary objective [3].

This section aims to critique shortcomings in current research that implements blockchain technology in ensuring highly secure systems for autonomous vehicles and to provide recommendations for privacy-preserving Self Sovereign Identity (SSI) system to securely manage the identity of the passengers and the vehicle. While these strategies are expected to bring security and privacy benefits, the risk of user insider trust could be elevated. Current studies implement user trust assessment through the use of user interaction. However, no comprehensive security model is developed to measure overall user trust once they are in the driving seat [20].

4.3. Inclusivity and Accessibility

In this efficacious scenario, the simplified set of U-R per V given in Table 1 provides means of acquiring HTIoV-VN category in the form of authorized digital personalized communication devices. The number of vehicles that can be secured to offer controlled access to N restricted front and rear facing seats corresponds to O-2-R being the total number of allowed vehicles that use the same road conditions and further totally ‘O’ occupies and sensitive Apps respectively. In the light of this research regarding accessibility and inclusion, HTIoV-V is thoroughly veri now and new unique cognitive security components can provide ever new means of communications-sensory technology. The in-vehicle space is defined so that the

Inter-User verification between the communicating agents and the investigator (In-Vehicle Person) is systematic in the HTIoV-System, to accomplish appropriate formal HTIoV-V Capturing from the IoT-embedded (Internet of Vehicle) interactive entities [18].

To deal with a highly restricted solution proposed in, we envisaged and conceptualized a not extensive HTIoV-SAC-based systematic approach to develop a centralized Access to Control (A2C) system. Here, the emphasis is on designing one identifying device—HTIoV-Verification (HTIoV-V)—to allow various category user and In-Vehicle Person (IVP) nodes to access HTIoV-SAC Carrier-Controlled in VW-Lan equipped vehicles. The HTIoV-V User-Impaired are digital devices having processing recursive and interactive capabilities. Associating IVP vehicle-infrastructure with vehicular ad-hoc network means networking with wireless signals—transducer re-quits and hence, IoT-embedded Systems require Wireless Sensors and Actuators to raise valid access keys for new intruder entities of IoT-embedded systems which are digitally assembled. Specifically for verifying the user-on-u-owned personal IoTs, that are claimed to be part of the vehicle, Local Markets (LMs) are deployed in the Internet of Things (IoT). The HTIoV-V Agent Interposed within a carry-IP by the VAA-Persons (The general users and motor- and hearing-impaired drivers) emulates an implicit-User-Activity (U-Activity) predicated by any attribute of the HSign (HCI-Sounds and GSM (Global System for Mobile Communication) Signals) in the same meeting with specialized

The accessible design of HTIoVACS will allow people with disabilities to have secure access to self-drive vehicles [1]. Accessibility for motor, hearing, and visually impaired users is the chief consideration for the inclusive design. This design targets and addresses the essential security and privacy concerns raised in the extant literature of Internet of Things–IoT-connected and in-vehicle electronics with the Internet of Vehicles, (IoV). Accessibility considerations were comprehensively reviewed. However, devising the HTIoV-SAC-based devices to support user experience is a challenging task and it may be highly error-prone. The human authentication and access transactions for HTIoV-SAC Carrier-Authorized Door Lock Control are highly reliable if vehicle-infrastructure mechanism is delegated to support systematic door control for automated entities [21].

5. Case Studies and Best Practices

Most current access control authorization and authentication models provide convenient privileges to authenticated users based on their ID/password (or voucher code). However, these methods have security flaws and always require an administrator to maintain user accounts using an access control list (ACL) [5]. Nevertheless, administrators in connected smart vehicles are incapable of managing all authorized vehicles across the world, so a blockchain-based distributed multi-factor authentication model provides temporal and spatial access control strategies for an automated cloud-connected vehicle. Blockchain technology is considered the saviour of technologyhomologized worlds by dint of its distributed and decentralized architecture. It also provides trustworthiness in an untrusted environment, and has been widely applied to voucher issuance and auditing technology, such as Bitcoin, Ethereum, cryptocurrency and more. The model deploys a secure and efficient consensus algorithm to speed up the sharing of MFA data on a consortium blockchain, specifically designed for smart city vehicular environments. A notion of consensus is crucial for the quality service of vehicular networks, and different consensus algorithms offer a good deal of advantages to distributed ledgers in terms of reputation, network education, information reliability, performance, energy, conservation, etc. [9].

[22]Automated vehicles are no longer a mystical pipedream or the brainchild of sci-fi authors but are the products of cutting-edge technology, produced in factories and labs around the world. That is why, as with many other IoT applications, these driverless vehicles require multi-level access control systems to keep them safe from various cyber threats and attacks.

5.1. Existing Authentication Systems in Autonomous Vehicles

There are diverse adumbrations of vehicular IoT-connected vehicles (VIoT-connected vehicles) around the world. In the age of V-V, V-I, V-P infrastructure, the number of technologies interconnected devices and systems dramatically multiplies, and when they're built on open protocols, the security requirements need securely controlling the access to these smart environments. Front-end the huge world of VIoT, vehicular conglomerate systems can only be operated by the services comprising interacting devices with many diversified producers. There not only exist some governing entities where VIoT applications are released and monetised ("Tesla" onboard car entertainment advertising, auto-parking services, etc.) but also some entities that securely provide internet-based access to the cars and their internal devices/processes. Context key has shown to be a good estimator for the power of

commodities based on the consumption speed (light, intermediate or heavy) or for the measured distances and volumes (lengths, thicknesses, diameters, etc.) and it materialises, directe or indirectable, the state of some objects, or it gives the speed performance of an object or it determines a position (via observations made under some limits). We should look at it as any property that indirectly gives or directly characterises the state or the evolution of the studied object maximally expressible inside a proper interval of stability. Based on this formalisation of the context key, we realised a digital system of loyalty cards, when the purchases realized in different grocery stores enter into a common platform that computes the common gains (common promotions) and offers incentives. The advantages of such a platform are multiple: a global view of the possible advantageousness of soon shopping (that could contain promotions realized as the benefit of the chosen previous shops), transparency (clients feel some explanations for some not predominant but expensive promotions), the reward in terms of a store "expensive" promotion (slow acquisitions) and also the testing the more accessible and closest platform to help doors the other groceries [21].

5.2. Lessons Learned and Recommendations

Multi-factor authentication has a key role and is recommended for advanced IoT (A-IoT) applications to ensure security. Typically, multi-factor systems are tiered to have a second and sometimes third backup option when the first factor authentication is not possible. However, this complexity means multi-factor authentication can have the user experience compromised. This paper demonstrated a UAV video surveillance system, and proposed a user experience multi-factor model, aligning context-awareness (home, street or hazardous) with human perception, with good satisfaction but limited authentication security, to exploit functional versus weak attacks [5]. Future work for improving security should explore hybrid authentication features with more advanced techniques like blockchain to maintain user privacy and trust. Blockchain refers to a unique way of documenting and verifying trans-actions that automatically applies to decision-making procedure. It has become a secure tool in theoretical and practical situations beyond modeling and simulations in logistics and information technology, spilling over to web applications, supply chain management and inventory control. Blockchain ensures data integrity, traceability and nonrepudiation of all transactions, making it difficult for attackers to perform illicit activities without being remain simultaneously unverifiable [9].Wildcarders Blockchain model complements multi-factor

authentication with security questions about the user's profile. However, future work is necessary to implement this technique.

In their paper, "Human-Centric Authentication Systems for Secure Access Control in IoT-connected Autonomous Vehicles", the authors note that while access control is important for the security of IoT-driven AVs, authenticating users who should be granted access has become a struggle [1]. They demonstrate a prototype model and evaluate the performance of four different authentication approaches in a human-centric and vehicle-centric environment and provide other researchers with a starting point for developing and testing new authentication systems for connected AVs.

6. Security Frameworks and Standards

In this section, we discuss the potential security frameworks and standards that can be relevant for secure access control and secure data access in IoT-based digital technologies including smart cars [23]. In many countries, there are legal bodies involved in setting standards, such as Bureau of Indian Standards (BIS), Central Motor Vehicles Rules (CMVR), Transportation Research Board (TRB), and National Highway Traffic Safety Administration (NHTSA). In addition to this, in India, the government body for standardization is the BIS, which sets the standards for IoT. The security framework is the ECSA2 model, which permits an integrated view of the entire chargeable structure in Electric Vehicles; and Electric Vehicles Ecosystem In 2016, the European Union Agency for Cybersecurity (ENISA) published a report and a European Commission's Digital Single Market focusing on the EU Cybersecurity Act (2019) on the IoT where it not only poses strong end-to-end security threat that must be secured but it also emphasizes the fact that new device in the EU market should comply with these cybersecurity standards [24]. There are also standards formulated by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) that are to be applied to IoT. IEEE-P2413.1 working groups have developed standard protocols. This section deals with security frameworks (i.e. ISA 99, University Models, UCDAE) and standards (i.e. NIST, ISO/IEC, SEBABA, CMC, CSEC, and REGSBP) which are mainly set for ensuring secure communication of input/output data in V2X systems. In the open standard domain, IETF (Internet Engineering Task Force) has is a standard for secure communication referred to as IPSESA which is proposed for protection against Neural architectures to secure and manage IoT traffic. Another IETF standard named SCEAmVC and

EAE standards along with IEEE and ETSI standards are also identified by the researchers where the designs and typologies are taken for analysis, design, and test the effectiveness of the architecture in securing the IoT-based systems. For all level of communication, the well known Internet Protocol Security (IPSec) is used for device-to-device (network layer security), transport layer security (TLS), device to cloud, (Session Initiation Protocol) protective on demand and auto driving with and without piconet. Researchers have joined hands to make a secure edge framework for IT-enabled security. There are various type of security frameworks developed as described in the previous sections. For secure digital technologies and IoT-enabled systems, security is of utmost importance similar to Kerckhoffs' principles. From the point of view of the researchers, it has established diverse IoT-based systems and developed IoT enabled projects with full-time connectivity on a Cloud. We have been putting our bones in advance in developing a secure IoT model for more than four years. The researchers in were also looking at secure data access technologies and attributes like time, date, permission, information, data of the physical parameter, distance, place, and so on must be provided for security purposes. As various digital technology applications were developed, the security framework and standards must also be developed and deployed, like that of EC-Council's famous Cyber Security Framework which deals with IoT devices. Other such standards were ISO 18013-5 standard, that sets the baseline for digital driving licenses and work on Particle-based Renewable Energy as IoT and zero-carbon sustainable development. Such standards can be reviewed for this policy especially related to secure data access Technologies and oriented IoT-connected smart-cars other than the available defined IOT and Smart Vehicles Applications. Ocf and oneM2M are also two of the significant IoT consortiums. Security recommendations are given for smart autonomous vehicles and digital systems. The concept in this system is for more secure access control and secure data access in IoT connected Operational Technologies which might also be fitted in secure smart cars [25].

6.1. NIST Cybersecurity Framework

The Framework Core provides a set of activities to achieve specific cybersecurity outcomes. The Core consists of five functions—Identify, Protect, Detect, Respond, and Recover—each of which consists of specific categories, subcategories and thus controlling processes. In the context of access control considerations for IoT, the primary NIST characteristic area of concern is the Protect Domain [10]. The NIST Core specifies, in addition to the cybersecurity

objectives, the informative reference lists comprised of existing global standards and guidelines that could be useful for organizations in achieving specific cybersecurity outcomes. Each of the functions ties to a different general aspect of the security process, and this Framework has become highly influential in many countries for overseeing and regulating IoT and other secure systems that cut across all IoT networks organizations.

Security is key to guaranteeing the trust of users and the reliable operation of connected and autonomous cars [26]. The National Institute of Standards and Technology (NIST) is a U.S.-based agency responsible for establishing cybersecurity standards and best practice recommendations. In 2014, NIST released its Cybersecurity Framework, as a voluntary framework of standards, guidelines, and best practices based on existing standards, guidelines, and practices to help organizations manage cybersecurity risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach is based on risk management and provides a common language for cyber risk management within an organization and across sectors [7]. Figure 2 shows the five aspects of the Framework.

6.2. ISO/IEC 27001:2013 Standard

This article briefly studies 2.19 Pedantic Catalog of Countercloud Protection. The International EClix's worldwide headquarters located in international Lock using the company's server against the observer to ensure pristine functions. The pedantic catalog of opposition research focuses on different international agency identities and identification strategies. They're working on a Cloud Hypervisor Analysis Organization. He's making sure every trained cloud is operated in a virtual machine in iec. This service will be a good form of counter-defense against combat protection for international organization defenses.

IoT device endorsement and strong device authentication has been advanced through the application of the Protection Profile through the IEC/ISO 15408 standard. For these reasons, it is essential to implement an IoT allowance based on this reference system [27] [28]. This makes it possible to evaluate the security level of each device. In IoT project management, it is essential to ensure that the IoT elements comply with the push-to-complete standard requirement. The provision of independent and undeniable platforms and projects is essential for the local procedures defined by existing customers and the provisions of the International Organization for Standardization and the International EC. The property provides customers with the greatest benefits since virtually standardization ensures independence on the scale

of their projects, enabling technical choices to be reviewed by independent bodies to gain confidence, calculated by Subscriber authorities, to form fair connections with their competitors.

7. Integration with Access Control Mechanisms

The formulated goals should be the driving force behind the requirement for implementing an inherently secure IoT-connected autonomous vehicle access control system, which aids the user to access its resources reserved based on the basic access control system such as role-based access control (RBAC), employment-based access control (EBAC) of roles, attribute-based access control (ABAC) (employing fine-grained attributes), and capability-based access control (CBAC). Current state-of-the-art implementations of access control mechanism in the autonomous vehicle is proposed in. Where the human-centric access control mechanism in the implementation is applied by enforcing an advanced receiver-based social graph thereby deploying the leftover social relations in a vehicular network to estimate the trust between the users of the autonomous vehicle. Social network characteristics of a particular group of drivers (trusted or untrusted) are computed by using the matrix representation of the driver's contact information firstly and then the eigenvalues are dug out. The user trust between them is derived by using eigenvector.

The access control mechanism in an autonomous vehicle must provide the necessary security to address the safety and privacy concerns of all users; only then the environment can be considered secure. Integration between access control mechanisms and social networking has become a basic asset to monitor all security parameters of a system in real-time. In, a lightweight and robust two-level physical layer security system of an IoT network in an automotive application is proposed. This paper aims to minimize the malicious user transmission probability and maximize the power allocation divisor for the system to improve the transmission security of 5G-based wireless network. The social graph measures trust levels successfully, minimizing security vulnerabilities in the vehicular network. Concerns over unwanted access to and potential misuse of copious data have altered our goals of vehicular privacy aspects. To that end, a Privacy-Preserving Cloud-Assisted Access Control (PPCAAC) protocol with a hybrid cloud-powered authentication mechanism for IoT-connected autonomous vehicles is presented in. Access control mechanisms in the proposed

system not only manage the privacy preferences of all users but also protect the system from unauthorized access.

7.1. Role-Based Access Control

In our previous work, an attribute-based access control (ABAC) engine was added to our architecture in order to allow evolving IoT devices to seamlessly integrate new functionalities within the system thanks to more expressive policies [29]. RBAC was employed in the original system to dynamically authorize actors under the assumption of an initially fixed set of permissions corresponding to well-defined system roles. In this work, other access control mechanisms have been incorporated into the architecture. Access control in an ABAC is based on the participants' attributes (like age, height, education, job function, role or location) at the given system state with the additional possibility of having time functions to operate policies and to check the attributes of a participant within a certain time period [24].

Earlier access control used to be a mere means of authenticating and authorizing users into the system. During the early days of information security, access control was simply a matter of authenticating the user, and then the user obtained access to everything they needed to do their job. However, modern applications and access control requirements have changed considerably. Access control is supporting more user types and roles which means that it's no longer acceptable to open the floodgates for everyone; rather it's now very important to fine-grain all the data and system access accordingly [30]. Role-based Access Control (RBAC) manages the segregation of duties by tailoring privileged needs to appropriate roles based on job function representing distinct responsibility.

7.2. Attribute-Based Access Control

Since RBAC is based on roles, it can lead to role explosion, where for every possible role within the system there would be a set of permissionsets. To reduce the size of this permission set, it is proposed to use an attribute based access control (ABAC) model, where permissions are associated with attributes—user, device, and/ or context attributes. In this model, as is evident from its name, a user is associated with attributes corresponding to the role that he/she has. Therefore, since the list of attributes that a user has could be much smaller than the roles that a user has, ABAC could therefore scale horizontally more efficiently than RBAC [31].

A special case of the CAC model is Capability-Based Access Control (CapBAC). Each subject in the system gets a set of attribute-based capabilities. These capabilities fall within the authority limits associated with the subject, and the capabilities are horizontally scalable, as a result of which capabilities of different users could be more granular making them very useful in scenarios with large number of devices [32]. ABAC is another model that is widely catching up in IoT scenarios. Unlike RBAC, attributes are directly linked to the subject and object and privileges are directly associated with attributes. As a result, in addition to encouraging horizontal innovation in controlling the access, ABAC also encourages users directly associate new types of attributes with both resource (IoT device) and their secret and granted access frequency [33].

8. Future Trends and Emerging Technologies

Even if WiFi-Key schemecan be considered a valuable solution contributing to the IoT world, some doubts have been raised in the scientific community. Some issues related to the Wu et al.'s proposal seem to be negative. On the contrary, some limitations seem to be related to blockchain and to the number of transactions that need to be accepted by the system. According to Tseng and Lin, Wi-Fi-Key needs further refinements and reshaping. Blockchain is a distributed database technology that ensures security in the form of a digital ledger. It is a consensus-based algorithm that confirms transactions from users. However, blockchain can effect a delay in processing transactions, which affects latency directly. The use of blockchain technology is costly. The computing resources for executing and optimizing transactions are high, and storage is not feasible as an embedded IoT device Therefore, to mitigate that, a research interest is completely turning towards creating an image as new and attractive approaches. Many image authentication techniques have been proposed in real-time user identification systems. The radio frequency (RF) is one of the most common and new proposed techniques for user authentication in the IoT world now. The RF fingerprint from Wi-Fi signals is becoming increasingly popular in the perception layer, which will be used in future authentication process supports AVer in the paradigm of the Internet of Things.

[13] [34] [35]Moreover, image authentication is the most adopted and attractive topic in future research. Adopting perception layer for authentication in the IoT supporting AVer is a new approach, which opens a new research direction. Furthermore, some other researchers intend to explore blockchain-based authentication for the IoT. They propose a lightweight key

distribution scheme named WiFi-Key. It uses Wi-Fi physical layer features and smart contracts. They claim that Wi-Fi-Key can achieve a high level of security and so be an ideal communication solution for MCU-based and IoT applications.

8.1. Machine Learning and AI in Authentication Systems

When the vehicle ends up in a cold start, nothing is known about the services the vehicle will need next. Therefore, security must be provided as quickly as possible, which means that the IoT vehicle should initially accept almost any user, but as quickly as possible converge its view about its passengers and exclude every nonauthetic and unauthorized wireless traffic entering into the cabin. Later, if the same IoT vehicle needs to be used while the engine is still off, the situation is similar to the previous discussion, but with some additional physical access control measure like the attitudes to be assumed by the self-driving vehicle towards people like pedestrians, cars, and bicycles. This is crucial in the context of vehicle sharing, where they can be utilized in public places for some hours. Even later, we can imagine to use refined modalities such as one-time passwords based on biometrics and a huge amount of traffic data (window traces using the previous example), if we imagine to run fully customizable applications inside the cars. All these scenarios can be seen as partial steps towards increasing the total engine-on lifetime blue backlog [13].

The modern vehicles not only serve as means of transportation but also behave as an important part of the IoT not only serve as means of transportation but but also connecting with other systems through the wireless network. In addition, In-Vehicle Infotainment (IVI) allows each passenger to having personalized experience, such as watching movies, listen to music, and so on. However, these fine-grained personalized data may be very useful for attackers. Here we specifically argue that the same physical vehicle may require different authentication approaches tailored to different services. After a certain service gets into the vehicle and meets its host system, initial configuration routines shall be initiated to give the initial constraints to the service, and then one or more authentication methods shall be launched both in host in opportune areas and in the service. The results of these steps should be filed into a consensus mechanism that should drive, in real-time the Cognitive FMN in deciding in real time which access control policy is the most advisable in the current context [36].

8.2. Blockchain Technology for Secure Identity Management

Blockchain technology can be used to integrate security, privacy, and integrity-preserving mechanisms for secure identity management. Blockchain technology is first adopted as an effective trust management function, driven by machine learning algorithms designed to protect against threats related to distributed denial-of-service (DDoS) attacks in IoT-based smart city scenarios [37]. Blockchain technology can also be utilized as a reliable network detection mechanism, facilitating global vehicle tracking and localization security. Additionally, attributes and parameters are integrated into the transportation system to protect the privacy of the end users, promoting secure and seamless vehicular communications . End-to-end security aspects from the business of intelligent transportation systems (ITS) are identified for securing autonomous vehicles, deepening the focus on blockchain technology. The work provides an in-depth overview of different blockchain technologies, elaborates blockchain as a decentralized digital tool, and discusses its state-of-the-art applications in both autonomous vehicles and the IoV. A use case specifically for blockchain technology in encrypting data exchange in autonomous vehicles is highlighted, after which both the secure identity management and forensic analysis of blockchain in autonomous vehicles is introduced [38]. A benchmark study identifies the limitations and potential further research in vehicle forensics currently riding on the blockchain, proposing new ideas for future research. A detailed analysis of the blockchain system for pseudonym management used in autonomous vehicles is then introduced. A study of the forensics system for pseudonym resource faults utilizing external external blockchain settings is proposed for reliable forensics of privacy-preserving communication-based pseudonym management in autonomous vehicles.

9. Conclusion and Future Directions

In the future, we will focus on the secret data associated with both Individuals in this technology that are generated through human verification processes including the application programs running on individual-driven products. The Human-Driven Authentication (H335GH) is designed on human-generated input applications to achieve secrecy of session. The individual in Smart City of Office # 2018, 2 Faithful Road (SO20182FR) requests human verification from individual when necessary along with application-built mechanism to decide whether the service is for individuals or for public and anonymous (144-ER) users. In this study, the computation power concept of cosmological difference among various history

of individual-birth is based on DPTAM q-bits many-body knowledge quanta space programs developed using available quantum computing technology. [3]

The security of IoT-network-based advanced future applications requires smart multi-function channels to be established using hidden resources in distinctive computing channels. In IoT-enabled smart assets, physical data protection introduces adversarial insider and outsider threats. We propose a comprehensive 'Blockchain-based vengeance on-line multi-function swarm intelligence Chosen Reflex Algorithm' to ensure multi-date verification of different data types by fitness fluid adjacency anti-black and Adversarial Swarm Non-Prime Strain also Raid tests. The blockchain technology can be embedded to manage data sharing requirements, roles-waived functionality and access handling in public-ledger Smart Machines in Smart Cities (SMIPS), wherein Building Management Systems (BMS) are universally connected across cities. The local and manufacturing algorithms Associated with Ch-search and Raid in existing Smart IoT blockchain under construct stipulated Strain provisioning for boot and re-booting of artificial agents. [39]

Security in IoT-connected Smart Autonomous Vehicles (ISAVs) is a foremost concern, because the IoT ecosystem makes it easy for outsider attackers to hack local and remote reservations and apply unwanted control and a range of malware poisoning. We hereby proposed a pragmatic Human-centric Context-aware Authentication Scheme (Hun-CAS) for robust and transparent safety verification of Human-Operated New Access (HONA) and Machine Authorization to HONA (MAHONA) /Machine-to-Machine access (M2M) sessions. The self-defense mechanism of the SCSI-Band-of-Trust (S-Bot)-based CAS supports locational, attitudinal, situational, and historical, and paramedical healthcare dataset access control and patient data sharing. The AI-based standard authentication algorithms can handle personalized, quick, transparent information detection while avoiding deep learning training biases.

10. References

[1] A. Ali, M. Ahmed, A. Khan, A. Anjum et al., "VisTAS: blockchain-based visible and trusted remote authentication system," 2021. ncbi.nlm.nih.gov

[2] Tatineni, Sumanth, and Anjali Rodwal. "Leveraging AI for Seamless Integration of DevOps and MLOps: Techniques for Automated Testing, Continuous Delivery, and Model Governance". Journal of Machine Learning in Pharmaceutical Research, vol. 2, no. 2, Sept. 2022, pp. 9-41, https://pharmapub.org/index.php/jmlpr/article/view/17.

[3] Prabhod, Kummaragunta Joel. "Advanced Machine Learning Techniques for Predictive Maintenance in Industrial IoT: Integrating Generative AI and Deep Learning for Real-Time Monitoring." Journal of AI-Assisted Scientific Discovery 1.1 (2021): 1-29.

[4] Tatineni, Sumanth, and Venkat Raviteja Boppana. "AI-Powered DevOps and MLOps Frameworks: Enhancing Collaboration, Automation, and Scalability in Machine Learning Pipelines." *Journal of Artificial Intelligence Research and Applications* 1.2 (2021): 58-88.

[5] A. Ometov, V. Petrov, S. Bezzateev, S. Andreev et al., "Challenges of Multi-Factor Authentication for Securing Advanced IoT (A-IoT) Applications," 2019. [PDF]

[6] P. Kumar Sadhu, V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Easy-Sec: PUF-Based Rapid and Robust Authentication Framework for the Internet of Vehicles," 2022. [PDF]

[7] I. Ali, S. Sabir, and Z. Ullah, "Internet of Things Security, Device Authentication and Access Control: A Review," 2019. [PDF]

[8] S. Danba, J. Bao, G. Han, S. Guleng et al., "Toward Collaborative Intelligence in IoV Systems: Recent Advances and Open Issues," 2022. ncbi.nlm.nih.gov

[9] V. R. Kebande, F. M. Awaysheh, R. A. Ikuesan, S. A. Alawadi et al., "A Blockchain-Based Multi-Factor Authentication Model for a Cloud-Enabled Internet of Vehicles," 2021. ncbi.nlm.nih.gov

[10] S. Loredana Nita and M. Iulian Mihailescu, "Elliptic Curve-Based Query Authentication Protocol for IoT Devices Aided by Blockchain," 2023. ncbi.nlm.nih.gov

[11] J. Li, J. Jin, L. Lyu, D. Yuan et al., "A Fast and Scalable Authentication Scheme in IoT for Smart Living," 2020. [PDF]

[12] K. Istiaque Ahmed, M. Tahir, M. Hadi Habaebi, S. Lun Lau et al., "Machine Learning for Authentication and Authorization in IoT: Taxonomy, Challenges and Future Research Direction," 2021. ncbi.nlm.nih.gov

[13] P. Nespoli, M. Zago, A. Huertas Celdrán, M. Gil Pérez et al., "PALOT: Profiling and Authenticating Users Leveraging Internet of Things," 2019. ncbi.nlm.nih.gov

[14] W. Yang, S. Wang, N. Masri Sahri, N. M. Karie et al., "Biometrics for Internet-of-Things Security: A Review," 2021. ncbi.nlm.nih.gov

[15] P. Shen Teh, A. Beng Jin Teoh, and S. Yue, "A Survey of Keystroke Dynamics Biometrics," 2013. ncbi.nlm.nih.gov

[16] S. Uppuluri and G. Lakshmeeswari, "Secure user authentication and key agreement scheme for IoT device access control based smart home communications," 2022. ncbi.nlm.nih.gov

[17] M. Grobler, R. Gaire, and S. Nepal, "User, Usage and Usability: Redefining Human Centric Cyber Security," 2021. ncbi.nlm.nih.gov

[18] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A Survey of Internet of Things (IoT) Authentication Schemes †," 2019. ncbi.nlm.nih.gov

[19] P. Xiong, S. Buffett, S. Iqbal, P. Lamontagne et al., "Towards a Robust and Trustworthy Machine Learning System Development: An Engineering Perspective," 2021. [PDF]

[20] M. Elkhodr, S. Shahrestani, and H. Cheung, "The Internet of Things: New Interoperability, Management and Security Challenges," 2016. [PDF]

[21] S. Duque Anton, D. Fraunholz, C. Lipps, K. Alam et al., "Putting Things in Context: Securing Industrial Authentication with Context Information," 2019. [PDF]

[22] N. Singh, R. Buyya, and H. Kim, "Securing Cloud-Based Internet of Things: Challenges and Mitigations," 2024. [PDF]

[23] M. Umar Aftab, A. Oluwasanmi, A. Alharbi, O. Sohaib et al., "Secure and dynamic access control for the Internet of Things (IoT) based traffic system," 2021. ncbi.nlm.nih.gov

[24] M. Gupta, J. Benson, F. Patwa, and R. Sandhu, "Secure Cloud Assisted Smart Cars Using Dynamic Groups and Attribute Based Access Control," 2019. [PDF]

[25] P. Gaba, R. Shringar Raw, O. Kaiwartya, and M. Aljaidi, "B-SAFE: Blockchain-Enabled Security Architecture for Connected Vehicle Fog Environment †," 2024. ncbi.nlm.nih.gov

[26] R. H. Hsu, J. Lee, T. Q. S. Quek, and J. C. Chen, "Reconfigurable Security: Edge Computing-based Framework for IoT," 2017. [PDF]

[27] P. Kumar Sadhu, V. P. Yanambaka, and A. Abdelgawad, "Internet of Things: Security and Solutions Survey," 2022. ncbi.nlm.nih.gov

[28] K. Gopalakrishnan, A. Balakrishnan, K. Govardhanan, and S. Selvarasu, "Propositional Inference for IoT Based Dosage Calibration System Using Private Patient-Specific Prescription against Fatal Dosages," 2022. ncbi.nlm.nih.gov

[29] Y. Zhang and X. Wu, "Access Control in Internet of Things: A Survey," 2016. [PDF]

[30] T. Mawla, M. Gupta, S. Ameer, and R. Sandhu, "The ACAC_D Model for Mutable Activity Control and Chain of Dependencies in Smart and Collaborative Systems," 2023. [PDF]

[31] D. Chamorro and G. Vergara-Hermosilla, "Lebesgue spaces with variable exponent: some applications to the Navier-Stokes equations," 2023. [PDF]

[32] R. Xu, Y. Chen, E. Blasch, and G. Chen, "BlendCAC: A BLockchain-ENabled Decentralized Capability-based Access Control for IoTs," 2018. [PDF]

[33] R. Xu, Y. Chen, E. Blasch, and G. Chen, "A Federated Capability-based Access Control Mechanism for Internet of Things (IoTs)," 2018. [PDF]

[34] S. Paiva, M. Abdul Ahad, G. Tripathi, N. Feroz et al., "Enabling Technologies for Urban Smart Mobility: Recent Trends, Opportunities and Challenges," 2021. ncbi.nlm.nih.gov

[35] Y. Chen, X. Wang, Y. Yang, and H. Li, "Location-Aware Wi-Fi Authentication Scheme Using Smart Contract," 2020. ncbi.nlm.nih.gov

[36] H. Fang, A. Qi, and X. Wang, "Fast Authentication and Progressive Authorization in Large-Scale IoT: How to Leverage AI for Security Enhancement?," 2019. [PDF]

[37] T. Liu, F. Sabrina, J. Jang-Jaccard, W. Xu et al., "Artificial Intelligence-Enabled DDoS Detection for Blockchain-Based Smart Transport Systems," 2021. ncbi.nlm.nih.gov

[38] O. Cheikhrouhou, I. Amdouni, K. Mershad, M. Ammi et al., "Blockchain for the Cybersecurity of Smart City Applications," 2022. [PDF]

[39] U. Khalil, O. Ahmed Malik, M. Uddin, and C. L. Chen, "A Comparative Analysis on Blockchain versus Centralized Authentication Architectures for IoT-Enabled Smart Devices in Smart Cities: A Comprehensive Review, Recent Advances, and Future Research Directions," 2022. ncbi.nlm.nih.gov