Article

A Blockchain-Based Multi-Factor Authentication Model for a Cloud-Enabled Internet of Vehicles

Victor R. Kebande [1,2,†], **Feras M. Awaysheh** [3,*,†], **Richard A. Ikuesan** [4], **Sadi A. Alawadi** [5] **and Mohammad Dahman Alshehri** [6]

1 Department of Computer Science, Electrical & Space Engineering, Luleå University of Technology, 97187 Luleå, Sweden; victor.kebande@ltu.se
2 Department of Computer Science (DIDA), Blekinge Institute of Technology, 37179 Karlskrona, Sweden
3 Institute of Computer Science, Data Systems Research Group, Tartu University, 51009 Tartu, Estonia
4 Cyber and Network Security Department, Community College Qatar, Doha 00974, Qatar; richard.ikuesan@ccq.edu.qa
5 Department of Information Technology, Uppsala University, 75236 Uppsala, Sweden; sadi.alawadi@it.uu.se
6 Department of Computer Science, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia; alshehri@tu.edu.sa
* Correspondence: feras.awaysheh@ut.ee
† These authors contributed equally to this work.

Abstract: Continuous and emerging advances in Information and Communication Technology (ICT) have enabled Internet-of-Things (IoT)-to-Cloud applications to be induced by data pipelines and Edge Intelligence-based architectures. Advanced vehicular networks greatly benefit from these architectures due to the implicit functionalities that are focused on realizing the Internet of Vehicle (IoV) vision. However, IoV is susceptible to attacks, where adversaries can easily exploit existing vulnerabilities. Several attacks may succeed due to inadequate or ineffective authentication techniques. Hence, there is a timely need for hardening the authentication process through cutting-edge access control mechanisms. This paper proposes a Blockchain-based Multi-Factor authentication model that uses an embedded Digital Signature (MFBC_eDS) for vehicular clouds and Cloud-enabled IoV. Our proposed MFBC_eDS model consists of a scheme that integrates the Security Assertion Markup Language (SAML) to the Single Sign-On (SSO) capabilities for a connected edge to cloud ecosystem. MFBC_eDS draws an essential comparison with the baseline authentication scheme suggested by Karla and Sood. Based on the foundations of Karla and Sood's scheme, an embedded Probabilistic Polynomial-Time Algorithm (ePPTA) and an additional Hash function for the P_i generated during Karla and Sood's authentication were proposed and discussed. The preliminary analysis of the proposition shows that the approach is more suitable to counter major adversarial attacks in an IoV-centered environment based on the Dolev–Yao adversarial model while satisfying aspects of the Confidentiality, Integrity, and Availability (CIA) triad.

Keywords: blockchain; multi-factor authentication; access control; internet of vehicles; cloud-enabled systems

1. Introduction

Blockchain technology establishes a creditworthy ecosystem among independent participants within a non-trustable distributed environment according to Li [1]. For example, in the cybersecurity world, blockchain technology has very distinctive use-cases driven by the fact that many of the security parameters used for identification, authentication, and authorization in organizations have become progressively penetrable. With the introduction of different cloud-based applications, Bring Your Own Device (BYOD) [2], as well as other cloud technologies authentication challenges, continue to introduce several threat vectors to many organizations. Furthermore, the answers on dealing with identity management, authentication, and access-control security in the many heterogeneous environments constitute diverse challenges to many industries. Things-enabled communications, such as

Internet of Things (IoT) and Internet of Vehicles (IoV), for instance, are particularly affected by this authentication challenge. However, with the IoT becoming increasingly crucial to intelligent transportation system stakeholders, including cloud-based vehicular (VC) and IoV paradigms, greater threat vectors are continually introduced. This new trend involves communication and data exchange between several objects within different layers of control in centralized [3] and decentralized models [4]. Security, particularly the authentication mechanism, in such a deployment, it is pivotal to realize the general IoT vision. Exploring the potentials of blockchain technology applications was a subject of intensive discussion in the literature. Many researchers investigate its ascribed advantages beyond the premises of cryptocurrencies. Among these possible applications, Blockchain-driven access control has distinguished itself as a promising trend [5,6].

Due to the dynamic nature of access control, agility has become unavoidable in many domains, including the connected vehicles [7]. For this, several studies have proposed access control technologies to address the broader intelligent transportation systems [8] due to ease of use and simplicity with an adequate security level [9]. Access control mechanism such as single sign on (SSO), Multi-Factor Authentication (MFA) process, Open Authentication (OAuth), open ID connect, as well other forms of authentication are key candidates in this context. With SSO, however, an entity can be authenticated using one set of login credentials and given access rights to multiple applications and services in a cloud platform to eliminate further prompts when the user switches applications or services during the same session. However, different organizations have opted to enforce MFA to verify a user's identity, requiring multiple identity and access management credentials. MFA can, therefore, be considered as a practical approach to security enhancement. Such models, however, required both security evaluation and risk assessment [10,11], as well as scalable security management frameworks [12].

Moreover, SSO and MFA have been implemented individually and not integrated to form Standard Operating Procedures (SOPs) in organizations. By leveraging the security strength of SSO and MFA combined, a viable alternative to entity authentication in things-enabled communication can be achieved, while minimizing the compromising limitation of each authentication mechanisms. The one good thing with SSO is that it can log user activities and monitor user accounts. The introduction of MFA in organizations, on the other hand, has been considered as one of the effective control measures that an organization can put in place to prevent attackers from gaining access to critical infrastructure as well as networks, thus preventing access to sensitive information. Accordingly, if a criminal manages to steal a user credential, he/she will be foiled by having to verify his identity differently. Hence, making it significantly hard for any adversary to steal legitimate user credentials for malicious activities on any organization network [13]. Besides SSO and MFA, security by design is a critical factor in the fortification of the system [14].

To further strengthen the security mechanisms and keep prevent attackers from malicious and unauthorized access, this study discusses a lightweight blockchain-based multi-factor authentication scheme for smart cities that integrates SSO and SAML in the cloud. This was motivated by the knowledge that IoT-based smart cities usually implement a complex distributed system that may involve multiple stakeholders, applications, sensors, as well as other IoT devices [15], hence the need for an integrated authentication mechanism. In addition to the aforementioned, this manuscript further extends the earlier work presented in [16].

1.1. Key Security Issues in IoV

The interaction between diverse applications and services across the vehicle cloud face a number of challenges. Among these challenges is the heterogeneity and the need to achieve inter-operable solutions. That notwithstanding, attackers can easily exploit vulnerabilities emanating from identity verification and device authentication in IoV. In order to enforce secure communication in a cloud-enabled IoV environment, the following are considered as key issues:

- Illegitimate identities where it is imperative to conduct a verification of key identities during authentication.
- Unauthorized access where it is important to verify the authenticity of a use accessing the cloud server or IoT device.

1.2. Contributions

Whilst several studies on authentication for IoT-based smart environments have leveraged the principle of MFA, the ultimate objective of any security mechanism is to guarantee secure communication by preventing compromise and attacks on the existing authentication mechanisms. Based on these factors, a secure MFA scheme for IoV ecosystems has been suggested. Therefore, the contributions of this paper are summarized as follows:

- The paper proposes a Multi-Factor Blockchain-based authentication model that uses an embedded Digital Signature (MFBC_eDS) for vehicular clouds and Cloud-enabled IoV.
- The suggested MFA Scheme combines and integrates a number of aspects in order to harden key authentication techniques. For example, SSO and SAML are key aspects that have been used to enhance authentication of IoT systems in the cloud. The security strength of the proposed approach shows that it satisfies the principle of data confidentiality and integrity, two cardinal components of the security of IoV.
- An embedded probabilistic polynomial Time Algorithm (ePPTA) with an additional hash function has been suggested that not only compliments the existing schemes but also hardens based on existing weaknesses, while it is applicable in an IoV-based environment.
- This study concentrates on addressing the degree of resistant-precisely on the possible failure of the mutual authentication phase, once P_i is generated.

1.3. Organization

The remainder of this paper is organized as follows: Section 2 presents the required background and motivation concepts behind this work. Section 3 presents existing state-of-the-art publications on related areas that we discuss in this manuscript. Section 4 exhibits the methodology used and the approach used that relies on the Karla and Sood authentication scheme and discusses its primaries. We introduce the proposed model in Section 5, alongside the validation process. A comprehensive discussion on this study's main findings took place and was discussed in Section 6. Finally, the study drafts its conclusions and future work in Section 7.

2. Background

This section explains the basic concepts and definitions of authentication models, single-sign-on frameworks, vehicular clouds, and the IoV paradigm.

2.1. Multi-Factor Authentication

A Multi-Factor Authentication (MFA) scheme offers solutions to the security risks and vulnerabilities found in a single-factor authentication mechanism. MFA thus offers security enhancement that allows a user to present two or more pieces of authentication credential when logging in to any account. This can range from something you know (password or PIN), something you have (smart card), or something you are (fingerprint) [17,18]. However, the latest MFA solutions incorporate additional factors which can consider context and behavior when authenticating a user—for instance, the location when logging in, attempted log-in time (such as late at night, for instance), the device being used (either a smartphone or a laptop), as well as the network being used to access (either private, public, or designated IP address range). With MFA, a complementary layer of security is added to strengthen the security against an attack [18]. A more robust (not necessarily complex) authentication often poses a usability problem [19]. Therefore, there is the need to evaluate the usability of a security mechanism constantly. As a simple thumb rule, usability is inversely proportional to security. It is, therefore, essential to note that there is a trade-off between usability and security when it comes to deciding on authentication schemes. The username and password

authentication process is the most popular means, despite their security flaws because they are easy to implement and allows the user quick entry to the system. They can be implemented with less computational complexity, speed, and scalability [17]. Additional devices are required to implement an MFA, which could be expensive, and more computational complexity will be required, which also increases processing time.

2.2. Single-Sign On

With the availability of cloud computing platforms, users are now able to access multiple, heterogeneous systems, either on the Internet, Extranet, or Intranet [20]. However, access to multiple systems may also mean multiple login credentials that users need to possess. This process can add extra pressure on the user to create and remember multiple login credentials, usually in the form of usernames and passwords, as different systems (may) have different constraints [21,22]. Therefore, SSO addresses the problem of multiple login credentials for multiple systems [23]. It is an authentication scheme through which a server authenticates a user with a single set of login credentials to gain access to all or multiple system resources and services without being prompted for a repeated login process. The main benefit of the SSO is the provision of improved security and compliance. Figure 1 shows a simple classification of SSO depicting where and how it is deployed, the set of credentials, and protocols.
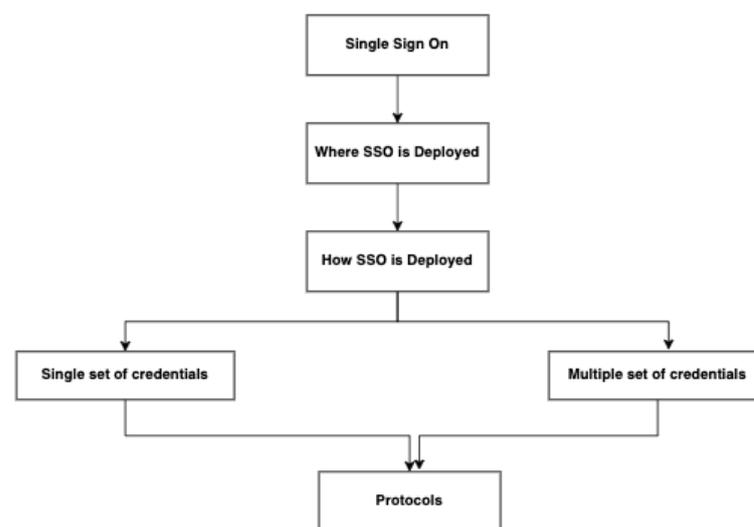
Figure 1. How SSO strategy is classified, where and how it is deployed.

In order to improve the security and usability of a system, SSO is usually deployed both within the Intranet, Extranet, and at the Internet level. However, a wide range of security vulnerabilities with the SSO approach exists [22]. For example, OpenID is a key technology that has been used by many Internet Service Providers (ISPs) as an authentication scheme for SSO [22]. To implement OpenID, one must integrate it with Secure Socket Layer (SSL) connections to leverage the RSA public-key cryptography of an SSL. The problem that comes with this measure is that there are high computational costs involved when cryptography is used [22], hence the need to refine and secure the SSO process while minimizing the computational costs. The use of SSO has led to information security vulnerabilities such as identity deception, identity theft, and authentication issues, especially in the cloud platforms, which mostly have seen a rise in Man in the Middle (MiTM) attacks or dictionary attacks. An SSO model for big data federation architectures was reported as well in [24] to depend on the reference model and digital evidence.

2.3. Vehicular Cloud

Vehicular Cloud (VC) refers to a group of broadly autonomous vehicles whose corporate computing, sensing, communication, and physical resources can be coordinated

and dynamically allocated to share internet access, as well as data, with other devices both inside and outside the vehicle. The VC can be formed by vehicles autonomously and provides a vast number of applications and services that can benefit the entire transportation system and its stakeholders (drivers, passengers, and pedestrians). This process, however, involves the use of onboard computational resources to facilitate communication and decode message and information storage. This concept of utilizing excessive onboard resources in the transportation system and the latest computing resource management technology in conventional clouds provides the substratum for the development of the VC. In general, it is composed of (i) Vehicular Ad-hoc Networks (VANET), where communication can be between vehicles (V2V) or vehicle and roadside infrastructure (V2I). (ii) Connected vehicles that interact with each other (V2V), the roadside infrastructure (V2I), and beyond (V2X) via wireless communications. (iii) VC is an attractive technology, which takes advantage of big data analytics [25] and cloud computing to support many novel applications. Like any other VANET, data privacy, entity authentication, and resource management are major challenges. Entity authentication and data privacy in such context are top priorities, maintaining its provenance [26].

3. Related Work

As an important method of hardening security, there has been a vast contribution in different authentication techniques in research that have provided essential solutions. An optimization approach focused on IoT security has been enforced with cryptographic encryption techniques for medical images using grasshopper and Particle Swarm Optimization (PSO). It depicted a diverse encryption algorithm for the secure transmission of medical images in an IoT environment [27]. Next, a lightweight authentication scheme has opted to focus on a multi-gateway for Wireless Sensor Networks (WSNs) in IoT—the proof of analysis of this scheme shows it prevents usual attacks [28,29]. Given that most IoT authenticating techniques use single-factor techniques, research by [30] has proposed a lightweight MFA for IoT devices that configures physical functions within IoT devices, and it makes use of very few cryptographic processes while employing a one-way hash. Another novel proposition protocol uses MFA for passwords, smart-cards, and bio-metrics for healthcare applications where there is a mutual authentication for each remote medical professional and the server [31].

Moreover, the authors in [32] have proposed an authentication scheme that focuses on cloud-IoT applications that are robust and lightweight. One advantage of this scheme is that it is robust against attacks with low computation overhead. Studies by Zisang et al. [33] have proposed a blockchain-based authentication approach for the Internet of Vehicles (IoV) that also manages key agreement protocols. In addition, in that study, blockchain is mainly used as a Trusted Authority (TA) that allows the management of the ledger that can store information related to the vehicle. It is also essential for the vehicles to perform mutual authentication with the TA through the intermediate node. However, the study pinpoints low computing overhead [33]. Another comparative study aimed at checking if blockchain technology can be used to improve the security, privacy, and trust of vehicle technology shows that blockchain could easily facilitate resource sharing among vehicles with a focus on computational, storage, and communication [34]. In addition, the study by [35] suggests an approach for solving security issues in IoVs for purposes of intelligent transport. Their study has a focus on communication, consensus-making, and authentication using a Byzantine consensus-based algorithm. From their study, the Byzantine outperforms the traditional authentication methods for IoV. Notably, that study mainly offers a key reference solution for authentication issues to the blockchain. While the ultimate benefits are decentralization, scalability, and fault-tolerance, it hardly has a focus on being integrated with multi-factor modalities [35].

Other relevant research includes an authentication scheme for IoV using blockchain that uses a blockchain ledger to design new nodes joining the consensus for vehicle identity. That authentication—which in the long run curbs malicious attacks [36]—is a blockchain-

based batch authentication that supports AI for IoV deployment—where, at the signing phase, the vehicle can broadcast messages to the Road Side Unit (RSU) using Vehicle to Vehicle (V2V) and batch authentication. The outcome is effective communication, storage, and computation cost and time [37]; in addition, an efficient blockchain authentication scheme that has a focus on fog computing for IoV named EASBF with five main phases: initializing, registering, mutual authentication, key exchange, consensus, and certificate update. EASBF uses elliptic curve cryptography and one-way as opposed to ePPTA being employed in this paper [38]. Lastly, blockchain-based lightweight for secured V2V uses blockchain and achieves data authentication among vehicles in real time for purposes of vehicle real-time adversary detection [39].

4. Methodology

We mainly focus on the authentication of secure communication between vehicle-to-vehicle (V2V) and vehicle-to-Cloud (V2C) as shown in Figure 2. The model comprises the following components:

- a set of connected smart vehicles;
- a peer-to-peer (blockchain-based topology) and IoT-to-Cloud network connected by multiple cloud service providers;
- a public Cloud infrastructure.
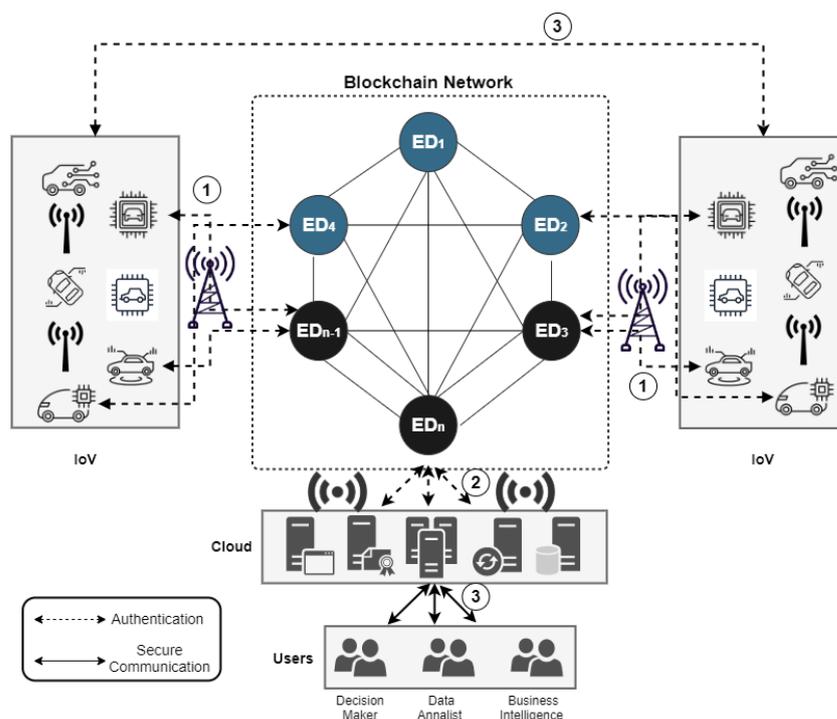
Figure 2. Blockchain-based Multi-Factor Authentication with ePPTA for IoV.

The connected vehicles collect sensor data using a solid-state programmable device, like real-time electricity load, temperature, proximity and humidity sensors, electricity consumption, . . . , etc. In our model, the connected vehicles send the ID of the corresponding cloud service providers to confirm their manager. Hence, at the data aggregator layer, the cloud service provider is responsible for several connected vehicles and maintaining the data-flows among the V2V and V2C in real-time. The proposed architecture in Figure 2 is further discussed, thus:

1. Initial Registration: when a vehicle joins the network and first participates in the system, it is asked to generate a hash-chain for the initial registration.

2.　Update the hash-chain Information: using one-time passwords, the vehicle periodically changes their hash-chains, so they need to contact the service provider to generate a new chain to establish a communication with the cloud.

3.　Communication establishes: a secure data channel is established (authenticated), V2V and V2C take place.

Approaches Based on Karla and Sood's Scheme

The Elliptic Curve Cryptography (ECC) in Karla and Sood [40] is based on the authentication protocols for the HTTP client that targets embedded devices. This protocol acts as a client, it is configured over TCP/IP, and it operates over a client/server communication with three distinct phases as is shown in the workflow protocol as follows: an embedded device (D_i) that wants to connect to the server (S) must register with the server (S), by first sending an identity, ID_i to S. Then, S will generate a key, P_i to be used coupled with a randomized number, and R_i that is to be used with the identity of the embedded device, D_i. This approach is computed as follows:

- Registration: D_i submits ID_i

$$T_i = H(R_i \oplus H(X))$$
$$A'i = A_j xG, T_i, ID_i$$
$$Ai = H(Ri \oplus H(X) \oplus Pi \oplus CK')$$
$$CK = H(R_i \parallel X \parallel \text{EXP-Time} \parallel ID_i)$$
$$Server\ Stores\ A'i = A_j xG, T_i, ID_i$$
$$Server\ generates\ P_i$$
$$x \longrightarrow S' private\_key$$
$$EXP - Time$$
$$S \longrightarrow \text{ sends } CK' to D_i$$

- Pre-Computation Time Phase
  Once D_i obtains the authenticating key CK', it becomes paramount that this can be used in the message computation that is required to be authenticated. A random number N_i is selected, which uses the authentication key CK' for computation as follows:

$$Select\ N_1$$
$$P_1 = N_1 xG$$
$$P_2 = H(N_1 xCK')$$
$$D_i\ sends\ required(\text{Auth})message(ID_i, P_1, P_2)$$

- Authentication Phase
  After the server, $S \longleftarrow (ID_i, P_1, P_2)$, it proceeds to such using ID_i, and it can find the desired record using the private key and expiration time $EXP - Time$ and the computation is as follows:

$$R_i = T_i \oplus H(X)$$
$$CK = H(R_i|X|EXP - Time|ID_i)$$
$$P'_2 = H(P_1 xCK)$$
$$S\ checks\ if\ P'_2 = P_2$$
$$Random\_number\ N_2\ is\ selected$$
$$Calculates\ ECC\ based\ on\ P_3 = N_2 \times G\ and\ P_4 = N_2 \times A'$$

The embedded device will then calculate values of A', checks if $P'_4 = P_4$ and then it sends a message to the server, S. Once the server checks if $V'_i = V_i$ a mutual authentication between D_i, a cloud server is generated and both parties agree on a common session key.

According to Karla and Sood's scheme [40], an attacker may only try to find intrusion mechanisms through unauthorized access and specifically by accessing the cloud server instead of an IoT device or an embedded device. As a result, Karla and Sood's [40] scheme will resist a replay attack, a man in the middle attack, eavesdropping, cookie theft, brute force attack, dictionary attack, verifier attack and mutual authentication, confidentiality, and anonymity. Based on Karla and Sood's work, we are more concerned with the degree of resistance if such a scheme is to be employed in a smart city and, as a result, the authors of this paper are more concerned with step 3 (mutual authentication phase) on possible failure once P_i is generated.

5. Proposed Lightweight MFA Scheme

This section presents the proposed Lightweight MFA Scheme by mainly exploring the adversary model and the lightweight blockchain-based Multi-Factor Authentication (MFA) scheme that integrates SSO and SAML in the cloud. We have formally defined BCMF_eDS supported access control model in Table 1 that shows the model's primary assets and functions. In addition, it describes the effective authentication scheme using the MFA and ePPTA foundations. A demonstration of the authentication and the associated decision process is presented in four steps. As shown in Table 1, IoV service permissions are the power set of the cross-products of the proposed algorithm and adapted approach. It worth mentioning that the system capitalizes on Phase-3, on the possible failure of the Karla and Sood [40] mutual authentication phase. In addition, this study also looks at the constitutes of the adversary model.

Table 1. Formal BCMF_eDS authentication Model Definitions.

Basic Sets and Functions

- Vh_i is a finite set of Vehicles that is ($i = 1, 2, \ldots, n$) and SP being the trusted service provider authority.
- P_uK and P_rK are the Public and Private keys of each Vh_i.
- H_i, R_{ID}, S_{ID}, and T_S are hash function, Real Identification, Secret Identification, and a Time Stamp, respectively.
- For any probabilistic polynomial time adversary, a probabilistic polynomial-time generates a T_S for each R_{ID} and S_{ID} by adding a new H_i for every Vh_i.
- T is an upper bounded set of a subset X of some preordered set ($T_K, \leq$) is an element of T_K which is greater than or equal to every element of X $\|\|$, and the size of the input for the T_S is $T_S(n) = O(n_k^T)$ for some positive constant k.
- The selection algorithm sort based on m integers performs Fm^2 operations for some constant F. Time is a polynomial time algorithm and runs in $O(m^2)$.
- ePPTA: common session set when $\{ePPTA \rightarrow H_i\}$. Formally, $H_i + R_{ID} + T_S + H_i$.
- Each Vh_i in the system maps P_rK, and ID in to a secret value.
- ePPTA: $H_i \cup R_{ID} \cup S_{ID} \cup T_S \{Request\} \rightarrow T_i = H(P_rK \oplus H(X))$: $\begin{cases} A'_i = A_j xG, T_i, ID_i \\ A_i = H(P_rK \oplus H(X) \oplus P_uK \oplus CK') \end{cases}$

Effective Authentication, MFA Based on ePPTA (Derived Functions)

- For each attribute att in ATT such that attType(att) = set:
  - $CK = H(P_rK\|X\|\text{EXP-Time }\|ID_i)$
  - Server Stores: $A'_i = A_j \times G, T_i, ID_i$
  - Server generates: $P_uK + S_x + Hsh$
  - $x \longrightarrow S'P_rK, \text{EXP\_Time} \|\| S \longrightarrow$ sends CK' to S_i
  - ePPTA $\rightarrow \begin{cases} \left(\frac{1}{2} - \frac{1}{2^{n+1}} < \frac{1}{2}\right) & \text{If the Algorithm is unsatisfiable} \\ \left(\frac{1}{2} - \frac{1}{2^{n+1}}\right) \cdot \left(1 - \frac{1}{2^n}\right) + 1 \cdot \frac{1}{2^n} = \frac{1}{2} + \frac{1}{2^{2n+1}} > \frac{1}{2} & \text{If there exists a satisfying assignment} \end{cases}$

Table 1. *Cont.*

Authorization Functions and Decision Made

1. Vh_i confirms the received timestamp T_S by checking if $|T_S - TS^*| \leq \Delta T_S$, where T_S^* is the reception time of μ (the message). If the condition does not hold, Vh_i stops further processing. Otherwise, Vh_i fetches $(R_I D_{Vh_x}, R_{Vh_x})$ of the vehicle Vh_i based on the received temporal identity $S_I D_{Vh_x}$

2. Vh_i checks that $P_u K + h(R_I D_{Vh_x} \| P_r K \| P_u k) \cdot R_u k + V_h \left(R_I D_{h_x^*} \| R_u K \| V'_{h_x} \| P_u k V_{hx} \| \ T_S 1 \right) \cdot V_h x'_1 = \text{Cert}^+_{V_h x}. P$.
   If it matches, Vh_i continues if the condition is satisfied. It rejects the request and cancels the authentication process.

3. Vh_i now retrieves $R_I d_{Vh_j}$ as $R_I d_{Vh_j} = R_I d^*_{Vh_j} \oplus h(R_{Vh_x} \| R_I D_{Vh_x} \| T_S 1)$ and generates
   $\text{Cert}'_{V_h} = \text{Cert}_{V_h} \oplus h(TID_{V_h x} \| s_{Vh_x, V_h} \| TS_2)$
   $TC_{V_h x} = B_{V_h x} \oplus h(R_I D_{Vh_x} \| TS_1 \| R_{V_h x}), C_{V_h x} = h(TC_{V_h x} \ \| TS_2) \oplus h(s_{Vh_x, V_h} \| TS_2 \| Sx_{V_h x} \| R_I d_{Vh_x}),$
   $X_i = h(Sx_{V_h x} \| s_{Vh_x}, V_h \| K'_1 \| C_{V_h x} \| R_{V_h} \| \text{Cert}_{V_h} \|)$
   $R_I d_{V_h} \| R_I d_{Vh_x} \| T_S 1 \| T_S 2)$, where the current timestamp is $T_S 2$, to send a key to establish a request
   $\mu = \langle TID_{V_h x}, X_i, \text{Cert}'_{V_h}, K'_1, C_{V_h x}, T_S 1 \ T_S 2 \rangle$ to Vh_x

4. Vh_i creates $S_x V_h x^{\text{new}} = S_x V_h x^* \oplus h(S_x V_h x \| R_I D_{Vh_x} \| R_{V_h x} \| T_S 1)$ and updates $Sx_{V_h x}$ with Sx_{Je}^{new} for $V_h x$ in its secure IoV environment.

5.1. Assumptions Based on the Dolev–Yao Adversary Model

The proposed adversary model is based on the Dolev–Yao [41] framework that is used in the analysis of security protocols. The adversary model is aimed at showing failures of the security goals: Confidentiality, Integrity, and Authentication (CIA), by relying on the assumptions that the adversary has a reason for the attack, what an adversary aims to achieve, as well as the capabilities of an adversary. Based on the Dolev–Yao adversary model, this study extrapolated the following assumptions [42,43]:

- Confidential or secret information being transmitted can be obtained through a passive attack process such as eavesdropping.
- An adversary can easily interfere with communication between two parties in a connected smart city or IoT environment.
- Sensor nodes can be interfered with or compromised in a bid to extract sensor data which can further compromise the confidentiality.
- Modification/tampering of digital information, a process which can compromise the integrity, potentially, and the availability of the data.

5.2. MFA Scheme

Based on the ECC's mutual authentication scheme by Karla and Sood as well as the capability of an adversary in the adversary model, we propose a lightweight block-chain based MFA scheme that integrates SSO and SAML in the cloud. The key agreement is further discussed in the subsequent subsection.

Deployment phase: The service provider controls the system components and smart objects before their deployment. For example, to register a V_h, the service provider implements the following processes.

First: Vh_i check the $P_u K + h(R_I D_{Vh_x} \| P_r K \| P_u k) \cdot R_u k + V_h(R_I D_{h_v^* \| R_u K} \| \| V'_{hx} \| P_u k_{Vhx} \| T_S 1) \cdot V_h x'_1 = \text{Cert}^+_{V_h x}. P$. If it matches, Vh_i continues if the condition is satisfied. It rejects the request and cancels the authentication process.

Second: Vh_i now retrieves $R_I d_{Vh_j}$ as $R_I d_{Vh_j} = R_I d^*_{Vh_j} \oplus h(R_{Vh_x} \| R_I D_{Vh_x} \| T_S 1)$ and generates $\text{Cert}'_{V_h} = \text{Cert}_{V_h} \oplus h(TID_{V_h x} \| s_{Vh_x, V_h} \| TS_2) \ TC_{V_h x} = B_{V_h x} \oplus h(R_I D_{Vh_x} \| TS_1 \| R_{V_h x}),$ $C_{V_h x} = h(TC_{V_h x} \ \| TS_2) \oplus h(s_{Vh_x, V_h} \| TS_2 \| Sx_{V_h x} \| R_I d_{Vh_x}), X_i = h(Sx_{V_h x} \| s_{Vh_x}, V_h \| K'_1) +$ $(\| C_{V_h x} \| R_{V_h} \| \text{Cert}_{V_h} \| \ R_I d_{V_h} \| R_I d_{Vh_x} \| T_S 1 \| T_S 2)$, where the current timestamp is $T_S 2$, to send a key to establish a request $\mu = \langle TID_{V_h x}, X_i, \text{Cert}'_{V_h}, K'_1, C_{V_h x}, T_S 1 \ T_S 2 \rangle$ to Vh_x.

Moreover, the service provider also loads the shared secrets S_x of the vehicles associated with the certificate to advance the embedded digital signature.

5.2.1. MFA Key-Agreement Phases

The key agreement phases in this context are executed between the users (P and Q) in an IoT-based environment through an end-to-end communication, and this is achieved based on the following step, leveraging the embedded Probabilistic Polynomial-Time Algorithm (ePPTA).

- Step 1: Authentication Request. User P (IoT device) instantiates a communication link to the server, S, by sending the requisite identification parameters (DA).
- Step 2: Registration with ePPTA and Computation. Server generates P_i and R_i, which acts as a private key based on the following ePPTA mechanism.
    - An embedded Probabilistic polynomial Time Algorithm is applied to the DA and a new Hash for every P_i
    - A common session key is generated by both parties by relying on $P_i + D_s + Hsh$
- Step 3: Authentication Phase. Server transmits to ID and it is able to get any record

5.2.2. MFA Based on ePPTA

Based on the key agreement, we propose an integrated/embedded Probabilistic Polynomial-Time Algorithm (PPTA)-adding Digital Signature, D_s and a hash, Hsh, for every P_i generated by S. Based on this, a strong P_i that an adversary may not be able to interrupt is presented as follows:

$$T_i = H(R_i \oplus H(X))$$
$$A'_i = A_j xG, T_i, ID_i$$
$$Ai = H(Ri \oplus H(X) \oplus Pi \oplus CK')$$
$$CK = H(R_i \parallel X \parallel \text{EXP-Time} \parallel ID_i)$$
$$\text{Server Stores } A'i = A_j xG, T_i, ID_i$$
$$\text{Server generates } P_i + D_s + Hsh$$
$$x \longrightarrow S' \text{ Private\_key}, EXP - Time$$
$$S \longrightarrow \text{ sends } CK' \text{ to } D_i$$

This implies that, during the authentication phase, where a mutual authentication between D_i and cloud server is generated and both parties agree on a common session key (newly generated) based on $P_i + D_s + Hsh$, which means that, when the embedded device calculates values of A' and then checks if $P'_4 = P_4$, it has to be generated using a unique hash digest has every time it is changed (integrated PPTA with a security parameter) as is shown in Figure 2. This further means that, in a blockchain environment, the generated Hsh will be three times stronger given that the probabilistic polynomial-time algorithm has to undergo another Hsh and this will be as follows:

Step 1: Signing Px using a Ds

$$Sender - privatekey, P_x \text{ is generated}$$
$$Server - generates \, P_i + D_s + Hsh$$
$$Message - signed \text{ using } P_x$$
$$Sender \text{ public key, } P_k\text{-generated}$$
$$Message \text{ decrypted using}$$
$$Sender's \, P_k \rightarrow P_i + D_s + Hsh$$

Figure 3 which represents the ePPTA with a security parameter that hardens the MFA is implemented in Step 3 of the blockchain-based IoV model that was previously highlighted in Figure 2. Specifically, the ePPTA gives an assurance of access-control, confidentiality, and integrity. This also relies on the consensus made to the nodes in the blockchain network. Figure 4 shows the channel where ePPTA security parameter is implemented.
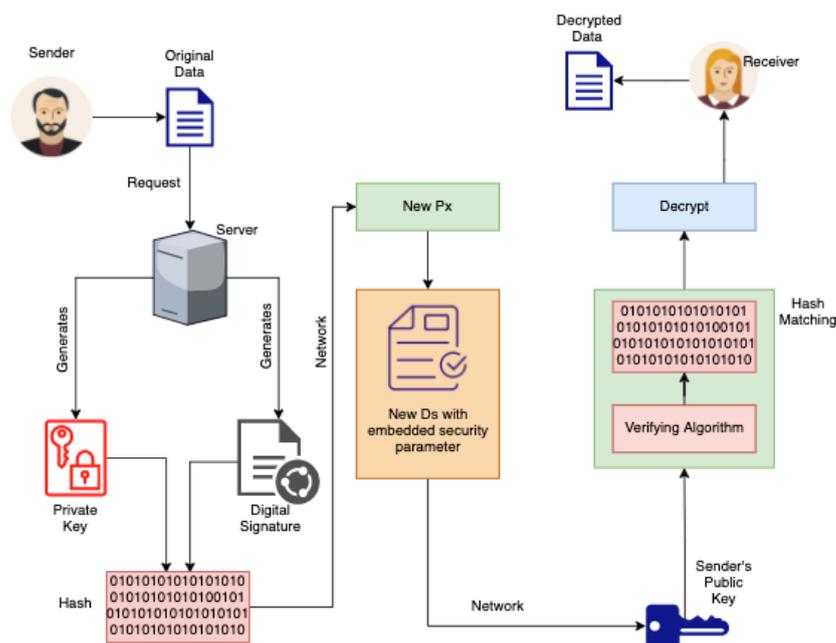
Figure 3. ePPTA with security parameter.
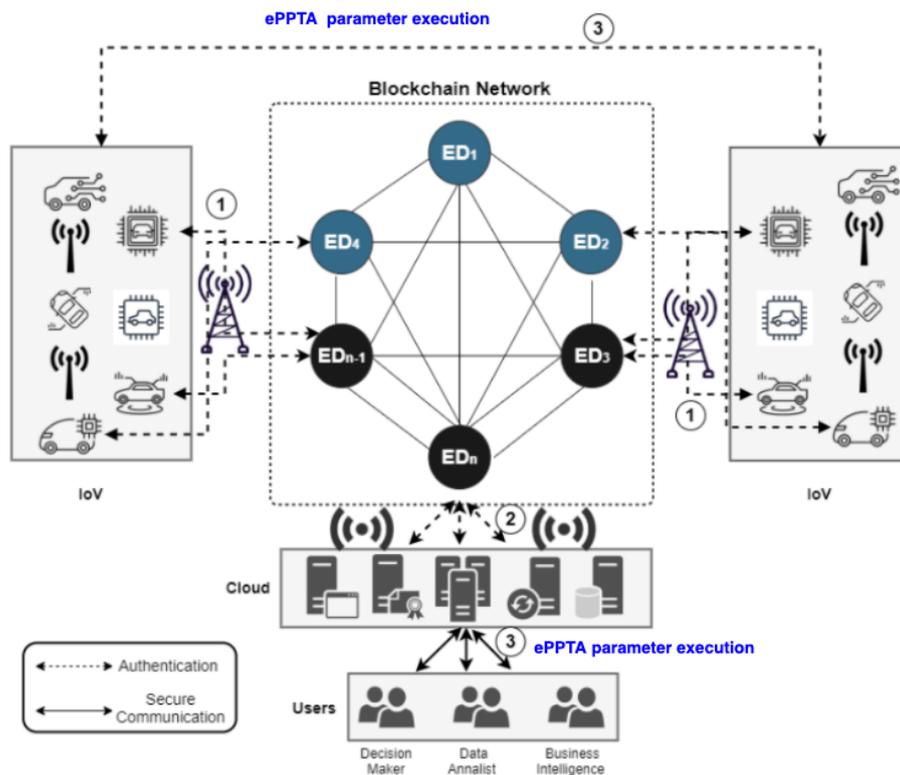
Figure 4. ePPTA with security parameter implementation in blockchain-based IoV.

Step 2: Apply step 1 to SSO-SAML

Through this step, the user can avoid further logins, and a directory of user details is maintained between the user and the Cloud Service Provider (CSP). The following requests are made in the SSO-SAML—$P_i + D_s + Hsh$ as follows: Supposing that a user wants to avoid multiple logins, it becomes imperative to maintain key details, which we posit as a Cloud Request, $C_{ij} - SAML$, and Cloud Application Request as $C_{App} - Rq$. The scheme requires the identification and authentication based on stored identities. For example, it

allows matching bivariate polynomials f($C_{ij} - SAML, C_{App} - Rq$) over some degree p as is shown in Equation (1):

$$f(C_{ij} - SAML, C_{App} - Rq) = \sum_{i,j=0}^{p} x_{i,j}(C_{ij} - SAML)^i, (C_{App} - Rq)^j (x_{i,j} = x_{j,i}) \quad (1)$$

This ensures that every user's identity can be requested based on the identity provider, IDP_{Rq}, which is mapped to the security parameter as follows:

$$IDP_{Rq} \longmapsto P_i + D_s + Hsh \quad (2)$$

For secure authentication, other relevant tasks accomplished in this step include Cloud Application Logging, $C_{App} - Log$, SAML Verification, VRF_{SAML}, and the user being able to access the cloud application, $USR_{Acc} - CApp$.

If there is a remote application, it can give the identity of the user based on the origin. In the context of this research paper, the origin may represent sub-domains used in the web or the IP addresses. The user is then able to be redirected to the IDP to request for authentication $Auth_{Rq}$. After this, the iDP can establish a logging connection over the browser section. An Authentication Response $Auth_{Rp}$ is built by the IDP which is represented by an XML-doc that consists of the user's detail. These details are then transferred to the CSP through the ACK_{sso} and Rly_{Tgt}. Eventually, the identity of the perceived cloud user can easily be established, and the CSP is able to transmit CSP_{Trsmn}. By employing this mechanism, the proposed approach can effectively prevent device/node hijacking as well as a spoofing attack within the communication channel.

The SSO service request and response occurs *n* and *m* number of times, respectively. This means that there may be distinctively *n* authentication modalities with *d* authenticating devices. Precisely, each authenticating modality possesses some characteristics c. We represent the authenticating modalities based on the characteristics as:

$$n = \{n_1, n_2 \ldots n_n\} \quad (3)$$

and also with the modalities characteristics as is shown in Equation (4)

$$n_c = \{c = 1, 2, \ldots n\} \quad (4)$$

The number of authenticating devices are represented as is shown in Equation (5)

$$d = \{d_1, d_2 \ldots d_n\} \quad (5)$$

Therefore, the total authenticating modalities, features, and authenticating devices with their characteristics are represented based on Equation (6) given some degree *p* as follows:

$$f(n_c, d) = \sum_{i,j=0}^{p} x_{i,j}(n_c)^i, (d)^j (x_{i,j} = x_{j,i}) \quad (6)$$

The process starts with a request from the service provider SP_{Rq} to the user, which allows the user to register with the authentication server. This is then followed by the transmission of an SSO request $Trsmn_{SSORq}$ and an acknowledgment ACK_{SSORq} to the identity provider and a request for key generation, $Keygen_{Rq}$ and ACK_{keygen} to the SSO agent. After this request, the SSO agent can easily generate either a public or a private key and then the agent can be able to send the public key to the authenticating server. Finally, the authenticating server can generate the signature.

Step 3: Apply the New digital signature to the Blockchain

We present a decentralized IoT smart city architecture that employs blockchain technologies that are centered on the multi-factor authentication approach mentioned

in Step 1. The proposed architecture distributes the New Ds, over transactions as a New_{Ds} $* Ds + Proof$-of-$work$ $(PoW) + Hash$, which makes it infeasible to compute to any non-participating member. This mechanism can, therefore, foil the classical MITM, which SSO mechanisms are largely vulnerable to.

Every smart city can easily participate in normal transactions and communication can easily be effective over the distributed network. Our architecture integrates all transactions by incorporating a secure blockchain that has multi-factor authentication protocols that integrate SSO and SAML in the cloud and $New_{Ds} * Ds + Proof$-of-$work(PoW) + Hash$. Most importantly, each transaction is hardened using the sequence shown in Figure 5.
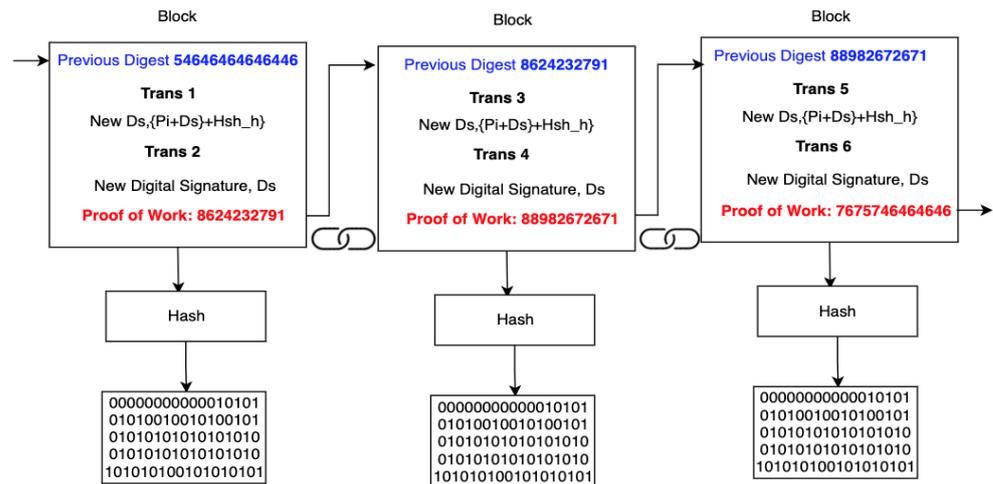
Figure 5. Figure depicting a Secure blockchain based on the current and new digital signature with a combined hash.

Each transaction $T = t_1, t_2, \ldots \ldots t_n$ on a given smart city blockchain is a validator that allows new members into the block to hold the new digital signature $New_{Ds} * Ds + Proof$-of-$work(PoW) + Hash$. This allows all the peers to validate the new peers using the most recent and longest Proof-of-Work. Unusual transactions that are not validated using $P_i + D_s + Hsh$ will be rejected. Peers can only be added to the blockchain network once a given transaction generates the P_x and P_k that are used during a normal transaction.

The PoW in the blockchain reduces the authentication and computation time needed from the scheme to the SAML SSO. It is worth noting that the proposed scheme can easily be applied to any blockchain system since it is secure in all means due to computational infeasibility of transactions because of immutable protocols. We also take note of the fact that the energy consumption by peers or attackers may be a point of interest in the blockchain. This study, therefore, prioritizes this as a major threat to the scheme. The new authentication scheme that is implemented in the blockchain is shown next:

$$T_i = H(R_i \oplus H(X)$$
$$A'i = A_j xG, T_i, ID_i$$
$$Ai = H(Ri \oplus H(X) \oplus P_i + D_s + Hsh \oplus CK')$$
$$CK = H(R_i \parallel X \parallel \text{EXP-Time} \parallel ID_i)$$
$$Server\ Stores\ A'i = A_j xG, T_i, ID_i$$
$$Server generates P_i + D_s + Hsh$$
$$x \to S'\ private - key, EXP - time(expiration\ of\ time)$$
$$S \longrightarrow \text{sends}\ CK'\ \text{to}\ D_i$$
$$Sender - private - key, P_x\text{-}generated$$
$$Server\ generates\ P_i + D_s + Hsh$$
$$Message - signed\ using\ P_x$$
$$Sender - public\_key, P_k\text{-}generated$$
$$Message - decrypted\ using\ Senders - P_k, P_i + D_s + Hsh$$

$$SSO\text{-}SAML + P_i + D_s + Hsh$$
$$New - D_s$$
$$Block: \; Trans_n + P_i + D_s + Hsh + PoW \rightarrow Hash$$

6. Discussion

As per the precise proposition that has been highlighted in this study, it is worth noting that the security techniques for an IoV are strengthened. The proposed mechanism of an embedded digital signature, which uses asymmetric encryption, aims to improve the PPTA from adversaries. Nevertheless, the proposed scheme follows an MFA technique that allows a user to authenticate several steps in the cloud while at the same time integrating with SAML-SSO. This approach is successful because there is a robust key generation procedure from the cloud server when an embedded device New Ds × Ds+Proof-of-work (PoW)+ Hash attempts to connect to the server, S. This is because an embedded digital signature is applied in the immutable ledgers in blockchain transactions. Consequently, several security factors have been taken into consideration, given that it is computationally complex to change the functional requirement of any block within the blockchain during the exchange of transactions and ledgers. This is mainly because the peers in a blockchain will tend to trust the longest PoW that is generated from the blockchain. This implies that our approach adds a security layer to the PPTA, making it computationally infeasible during an attack, thereby creating a significant degree of trust, confidentiality, and integrity.

The proposed approach holds a direct data privacy impact on IoT applications such as smart cities. The realization of smart cities depends on individual data privacy and security to ensure realizing its vision and widespread its adoption among practitioners. However, such a vision faces challenges that include privacy preservation with high dimensional data, securing a network with a large attack surface, establishing trustworthy applications, properly utilizing artificial intelligence, and mitigating failures cascading through the intelligent network [44]. It is also essential to pay attention to the privacy solution impact on the system's overall performance and employ state-of-the-art technologies like blockchain [45]. Further research directions utilizing our approach, hence, encourage further exploration of smart city deployment seeking privacy and performance.

A comparative analysis of the proposed approach with existing solutions is further given in Table 2. It can be observed that the proposed approach addresses key security objectives which were not considered in some earlier studies. Namely, we elaborate on data confidentiality and integrity. Further elaboration of these security objectives is discussed in the subsequent subsections.

Table 2. Overview of a comparative summary of attributes.

Attributes	Proposed	Karla and Sood	Melki et al.	Wu et al.	Sharma	Xu et al.	Chin
MFA	✓	X	✓	X	✓	✓	X
SAML-SSO	✓	X	X	X	X	X	X
Confidentiality	✓	✓	✓	X	✓	✓	✓
Integrity	✓	X	✓	✓	✓	✓	✓
Anonymity	✓	✓	✓	✓	✓	✓	✓
IoV-centered	✓	✓	✓	✓	✓	✓	✓
Blockchain	✓	X	X	X	X	X	X

6.1. Confidentiality

An adversary may want to intercept sensor data using various techniques, for example, through MiTM; however, the proposed scheme provides stronger approaches of an embedded digital signature that uses a private key, Px, and public key, Pk, to generate a new digital signature to compute the Proof-of-Work (PoW). Therefore, this implies that confidentiality is assured because any attempt by an adversary to eavesdrop on a communication would require a computationally complex attack path. Thus, attack during normal transactions in a decentralized smart city transaction can be said to be computationally

infeasible. Notably, if an adversary tries to eavesdrop, conduct a brute force, or change the immutability of the blockchain, an adversary will need to compute quadrillions of computations to generate the blockchain hash because the embedded process has New Ds × Ds + Proof-of-work (PoW) + Hash.

6.2. Data Integrity

The possible attack path of an adversary is hampered by the proposed scheme in this context. This is because an adversary would typically attempt to alter the signed message through falsifying the contents. However, in this scheme, this is not feasible because the proposed authentication scheme employs a double computation $BlockTrans_n + P_i + D_s + Hsh + PoW \rightarrow Hash$ which makes transactions unmodifiable in a blockchain. Additionally, this also defeats the MiTM attacks or a mining attack in which the blockchain miners posing as adversaries may decide to control the cluster heads. This type of attack has been addressed in several existing studies, as highlighted in Table 2. This study can be added to the list of other studies whose security schemes provide a mitigation against this form of attack.

Table 2 shows the security attributes of closely related schemes and they have been used to show the evaluation of the proposed scheme. The attributes have been used to show a comparative security analysis between the schemes by [28,29,32,40,41]. The proposed scheme is based on IoV and applied in a blockchain environment and integrates SSO-SAML, while it resists MiTM and DoS, by enforcing confidentiality, integrity, and anonymity. In addition, the proposed scheme is precise for it has less cryptographic computations of the New Ds × Ds + Proof-of-work (PoW) + Hash to allow less energy usage during blockchain computations.

Furthermore, the approach provides a tamper-proof free approach for the sensor data from sensor nodes which are more vulnerable to attacks. One potentially added advantage of the proposed approach is the reduction in human activity. By leveraging the seamless characteristics of the SSO, and the security strength of MFA schemes based on block chain, the proposed approach presents a manageable approach to implement effective security in smart cities. Given that IoV based systems require a greater degree of automation and seamless communication, the proposed approach is suitable for the current high-speed 5G interconnected smart cities. Whilst the integration of blockchain presents a conceptual drift towards autonomous security in an IoV-centered platform such as smart cities, there are numerous potential adoptions of this integrated security. For instance, as observed in [46], the implementation of IoT-enabled platform cuts across numerous domains, ranging from smart health, smart education, and smart homes to smart offices. By extension, therefore, this proposed approach can be leveraged in any IoV-based platform for a secure seamless automation process. In terms of security, this proposed approach provides a relatively similar security strength to previous studies. However, the flexibility and ease-of-use of security have been overlooked. Usable security is fundamentally a component of security that has proven to aid technology adoption and enhanced security [47–49]. Thus, within the context of an IoV platform, a usable security would require an effective authentication process that provides a seamless and time-limited operations for connected vehicles.

On the other hand, the power consumption in Edge deployment architecture is one of the main concerns, limiting a full expansion of large-scale data analytics over IoT models [50,51]. It is expected that, alongside addressing the security and privacy concerns, advances in energy consumption will lead to the development of cross-devices Edge Intelligence applications and architectures [52]. This is especially required in mobile edge applications and sensor mesh networks (e.g., wearable sensors). However, the power consumption in the connected vehicle's model is more resilient considering the vehicle's power capacity, unlike the edge side unites [53]. In this regard, the main focus of this study is pushing the current research status a step further, realizing a secure Edge Intelligence paradigm. Hence, by investigating cutting-edge technologies (e.g., blockchain-enabled IoV [54]) and well-established identification and access control technologies, we aimed at a resident, scalable, and secure IoV system.

6.3. Distributed Attacks

Blockchain technology is becoming increasingly attractive, affecting the next generation of large-scale distributed systems, providing the required privacy. The blockchain theory relies on storing information securely within the blocks of the blockchain's transactions. These decentralized consensus model transactions have the three main features: consistency, aliveness, and fault tolerance by nature [55]. However, in such an operational environment, distributed attacks are a leading concern [56]. Such an attack surface can return with transaction denial, as well as blockchain delay. Another attack dimension is punitive forking blockchain attacks where related transaction costs increased by peers in the blockchain, discouraging the production of non-renewable energy under certain circumstances [57]. The authors formalize the feather forking attack and we discuss how it can be applied in the smart grid context for the proposed purpose. They had further proposed a smart grid architecture addressing energy waste and production. In this context, we argue that combining the ePPT algorithm to the proposed blockchain-based identity and access control relieves such concern.

The proposed blockchain-powered approach enables different privacy-preserving models for IoT applications, such as data privacy, user privacy, location privacy, and privacy-preserving aggregation. Such a proposal aids in moving toward various advantageous features such as decentralization, anonymity, and audibility of the authentication process [58]. Hence, MFBC_eDS is a scalable and decentralized system with fast confirmation in the blockchain system. It uses a novel adaptive algorithm to integrate the Security Assertion Mark-up Language (SAML) to the Single Sign-On (SSO) capabilities. By combining these two strategies into an integrated consensus protocol, Blockchain smart contracts can be deployed as future work. This trend can capitalize on our proposed approach, strengthening against different threats, vulnerabilities, and attacks.

7. Conclusions

The integration of cloud computing and Vehicular Ad-hoc Networks (VANETs), namely, cloud-enabled IoV, has become a significant research area. This integration was proposed to accelerate the adoption of intelligent transportation systems. However, such a trend requires security mechanisms, ensuring data privacy, information integrity, and resource availability. In this paper, we explored the potential of a Blockchain-based Multi-Factor Authentication (MFA) model for the confidentiality and integrity of connected Internet-of-Vehicles (ioV). The proposed model integrates the Security Assertion Mark-up Language (SAML) to the Single Sign-On (SSO) capabilities for a connected ecosystem in the cloud. The evaluation reveals that the proposed model presents a reliable mechanism for enhancing the security of IoT-to-Cloud connected vehicles. In addition, this study presents the vision and need for robust access control in connected vehicle systems and fosters discussion on the identified future research agenda. We envision that this contribution will help achieve consensus among formal IoV access control models and real-world Cloud-Enabled IoV Platforms. As part of continuing work, parameters such as trust and malicious intention will be further explored to underscore the degree of reliability of the proposed solution. Device and user attribution within an IoV platform is another area of potential future work. Such future work involves developing several use-cases of malicious intention, where behavioral intentions can be modeled. The attribution process, on the other hand, can be used in a behavioral model. Taken together, therefore, the future work towards a reliable IoV authentication process would consider an extensive study of the uses cases that leverages behavioral model and attribution processes.

Institutional Review Board Statement: Not applicable

Informed Consent Statement: Not applicable

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

Abbreviations

The following abbreviations are used in this manuscript:

ICT	Information and Communication Technology
IoV	Internet-of-Vehicle
MFBC_eDS	Multi-Factor Blockchain-based authentication model that uses an embedded Digital Signature
MFA	Multi-Factor Authentication
SAML	Security Assertion Mark-up Language
SSO	Single Sign-On
VC	Vehicular Cloud
IoT	Internet of Things
BYOD	Bring Your Own Device
OAuth	open authentication
SOPs	Standard Operating Procedures
ISPs	Internet Service Providers
SSL	Secure Socket Layer
MiTM	Man in the Middle
VANET	Vehicular Ad Hoc Networks
V2I	Vehicle to Infrastructure
PSO	Particle Swarm Optimization
WSN	Wireless Sensor Network
TA	Trusted Authority
RSU	Road Side Unit
ECC	Elliptic Curve Cryptography
V_h	Vehicle
V2V	Vehicle to Vehicle
S	Server
D_i	Embedded Device
ID_i	Identity
N	Randomized Number
CK'	Authenticating Key
P_i	Key
$P_u K$	Public Key
$P_r K$	Private Key
H_i	Hash function
R_{ID}	Real Identification
S_{ID}	Secret Identification
T_S	Timestamp
$T_S(n) = O(n_k^T)$	size of the input for the T_S
$ePPTA$	Embedded Probabilistic Polynomial Time Algorithm
$EXP - Time$	Expiration Time
PoW	Proof of Work
New_{Ds}	New Digital Signature
Ds	Digital Signature

References

1. Li, Y. Emerging blockchain-based applications and techniques. *Serv. Oriented Comput. Appl.* **2019**, *13*, 279–285. [CrossRef]
2. Kebande, V.R.; Karie, N.M.; Venter, H. A generic Digital Forensic Readiness model for BYOD using honeypot technology. In Proceedings of the 2016 IST-Africa Week Conference, Durban, South Africa, 11–13 May 2016; pp. 1–12.
3. Alshehri, M.D.; Hussain, F.K. A centralized trust management mechanism for the internet of things (CTM-IoT). In Proceedings of the International Conference on Broadband and Wireless Computing, Communication and Applications, Barcelona, Spain, 8–10 November 2017; pp. 533–543.
4. Alshehri, M.D.; Hussain, F.; Elkhodr, M.; Alsinglawi, B.S. A Distributed Trust Management Model for the Internet of Things (DTM-IoT). In *Recent Trends and Advances in Wireless and IoT-enabled Networks*; Springer: Cham, Switzerland, 2019; pp. 1–9.
5. Ouaddah, A.; Abou Elkalam, A.; Ait Ouahman, A. FairAccess: A new Blockchain-based access control framework for the Internet of Things. *Secur. Commun. Netw.* **2016**, *9*, 5943–5964. [CrossRef]
6. Huang, J.; Kong, L.; Chen, G.; Cheng, L.; Wu, K.; Liu, X. B-IoT: Blockchain driven Internet of Things with credit-based consensus mechanism. In Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Richardson, TX, USA, 7–9 July 2019; pp. 1348–1357.
7. Gupta, M.; Awaysheh, F.M.; Benson, J.; Alazab, M.; Patwa, F.; Sandhu, R. An Attribute-Based Access Control for Cloud Enabled Industrial Smart Vehicles. *IEEE Trans. Ind. Inform.* **2020**, *17*, 4288–4297. [CrossRef]
8. Awaysheh, F.; Cabaleiro, J.C.; Pena, T.F.; Alazab, M. Big data security frameworks meet the intelligent transportation systems trust challenges. In Proceedings of the 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 5–8 August 2019; pp. 807–813.
9. Aladwan, M.; Awaysheh, F.; Cabaleiro, J.; Pena, T.; Alabool, H.; Alazab, M. Common security criteria for vehicular clouds and internet of vehicles evaluation and selection. In Proceedings of the 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 5–8 August 2019; pp. 814–820.
10. Aladwan, M.N.; Awaysheh, F.M.; Alawadi, S.; Alazab, M.; Pena, T.F.; Cabaleiro, J.C. TrustE-VC: Trustworthy evaluation framework for industrial connected vehicles in the cloud. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6203–6213. [CrossRef]
11. Elkhodr, M.; Alsinglawi, B.; Alshehri, M. A privacy risk assessment for the Internet of Things in healthcare. In *Applications of Intelligent Technologies in Healthcare*; Springer: Cham, Switzerland, 2019; pp. 47–54.
12. Alshehri, M.D.; Hussain, F.K. A comparative analysis of scalable and context-aware trust management approaches for internet of things. In Proceedings of the International Conference on Neural Information Processing, Istanbul, Turkey, 9–12 November 2015; pp. 596–605.
13. Kebande, V.R.; Alawadi, S.; Awaysheh, F.M.; Persson, J.A. Active Machine Learning Adversarial Attack Detection in the User Feedback Process. *IEEE Access* **2021**, *9*, 36908–36923. [CrossRef]
14. Awaysheh, F.M.; Aladwan, M.N.; Alazab, M.; Alawadi, S.; Cabaleiro, J.C.; Pena, T.F. Security by Design for Big Data Frameworks Over Cloud Computing. *IEEE Trans. Eng. Manag.* **2021**, 1–18. [CrossRef]
15. Chaturvedi, K.; Matheus, A.; Nguyen, S.H.; Kolbe, T.H. Securing spatial data infrastructures for distributed smart city applications and services. *Future Gener. Comput. Syst.* **2019**, *101*, 723–736. [CrossRef]
16. Karie, N.M.; Kebande, V.R.; Ikuesan, R.A.; Sookhak, M.; Venter, H. Hardening SAML by Integrating SSO and Multi-Factor Authentication (MFA) in the Cloud. In Proceedings of the 3rd International Conference on Networking, Information Systems & Security, Marrakech, Morocco, 31 March–2 April 2020; pp. 1–6.
17. Ramatsakane, K.I.; Leung, W.S. Pick location security: Seamless integrated multi-factor authentication. In Proceedings of the 2017 IST-Africa Week Conference (IST-Africa), Windhoek, Namibia, 31 May–2 June 2017; pp. 1–10.
18. Rehman, F.; Akram, S.; Shah, M.A. The framework for efficient passphrase-based multifactor authentication in cloud computing. In Proceedings of the 2016 22nd International Conference on Automation and Computing (ICAC), Colchester, UK, 7–8 September 2016; pp. 37–41.
19. Furnell, S. The usability of security–revisited. *Comput. Fraud Secur.* **2016**, *2016*, 5–11. [CrossRef]
20. Zhu, H.H.; He, Q.H.; Tang, H.; Cao, W.H. Voiceprint-biometric template design and authentication based on cloud computing security. In Proceedings of the 2011 International Conference on Cloud and Service Computing, Hong Kong, China, 12–14 December 2011; pp. 302–308.
21. An, Y.; Zaaba, Z.; Samsudin, N. Reviews on security issues and challenges in cloud computing. *IOP Conf. Ser. Mater. Sci. Eng.* **2016**, *160*, 012106. [CrossRef]
22. Radha, V.; Reddy, D.H. A survey on single sign-on techniques. *Procedia Technol.* **2012**, *4*, 134–139. [CrossRef]
23. Awaysheh, F.M.; Cabaleiro, J.C.; Pena, T.F.; Alazab, M. Poster: A pluggable authentication module for big data federation architecture. In Proceedings of the 24th ACM Symposium on Access Control Models and Technologies, Toronto, ON, Canada, 4–6 June 2019; pp. 223–225.
24. Awaysheh, F.M.; Alazab, M.; Gupta, M.; Pena, T.F.; Cabaleiro, J.C. Next-generation big data federation access control: A reference model. *Future Gener. Comput. Syst.* **2020**, *108*, 726–741. [CrossRef]
25. Awaysheh, F.M.; Alazab, M.; Garg, S.; Niyato, D.; Verikoukis, C. Big Data Resource Management & Networks: Taxonomy, Survey, and Future Directions. *IEEE Commun. Surv. Tutor.* **2021**, 1. [CrossRef]

26. Elkhodr, M.; Alsinglawi, B.; Alshehri, M. Data provenance in the internet of things. In Proceedings of the 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), Krakow, Poland, 16–18 May 2018; pp. 727–731.

27. Elhoseny, M.; Shankar, K.; Lakshmanaprabu, S.; Maseleno, A.; Arunkumar, N. Hybrid optimization with cryptography encryption for medical image security in Internet of Things. *Neural Comput. Appl.* **2018**, *32*, 10979–10993. [CrossRef]

28. Xu, L.; Wu, F. A lightweight authentication scheme for multi-gateway wireless sensor networks under IoT conception. *Arab. J. Sci. Eng.* **2019**, *44*, 3977–3993. [CrossRef]

29. Wu, F.; Xu, L.; Kumari, S.; Li, X.; Shen, J.; Choo, K.K.R.; Wazid, M.; Das, A.K. An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment. *J. Netw. Comput. Appl.* **2017**, *89*, 72–85. [CrossRef]

30. Melki, R.; Noura, H.N.; Chehab, A. Lightweight multi-factor mutual authentication protocol for IoT devices. *Int. J. Inf. Secur.* **2019**, *19*, 679–694. [CrossRef]

31. Dhillon, P.K.; Kalra, S. Multi-factor user authentication scheme for IoT-based healthcare services. *J. Reliab. Intell. Environ.* **2018**, *4*, 141–160. [CrossRef]

32. Sharma, G.; Kalra, S. A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications. *J. Inf. Secur. Appl.* **2018**, *42*, 95–106. [CrossRef]

33. Xu, Z.; Liang, W.; Li, K.C.; Xu, J.; Jin, H. A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles. *J. Parallel Distrib. Comput.* **2021**, *149*, 29–39. [CrossRef]

34. Mendiboure, L.; Chalouf, M.A.; Krief, F. Survey on blockchain-based applications in internet of vehicles. *Comput. Electr. Eng.* **2020**, *84*, 106646. [CrossRef]

35. Hu, W.; Hu, Y.; Yao, W.; Li, H. A blockchain-based Byzantine consensus algorithm for information authentication of the Internet of vehicles. *IEEE Access* **2019**, *7*, 139703–139711. [CrossRef]

36. Wang, X.; Zeng, P.; Patterson, N.; Jiang, F.; Doss, R. An improved authentication scheme for internet of vehicles based on blockchain technology. *IEEE Access* **2019**, *7*, 45061–45072. [CrossRef]

37. Bagga, P.; Sutrala, A.K.; Das, A.K.; Vijayakumar, P. Blockchain-based batch authentication protocol for Internet of Vehicles. *J. Syst. Archit.* **2021**, *113*, 101877. [CrossRef]

38. Eddine, M.S.; Ferrag, M.A.; Friha, O.; Maglaras, L. EASBF: An efficient authentication scheme over blockchain for fog computing-enabled internet of vehicles. *J. Inf. Secur. Appl.* **2021**, *59*, 102802.

39. Kamal, M.; Srivastava, G.; Tariq, M. Blockchain-based lightweight and secured v2v communication in the internet of vehicles. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 3997–4004. [CrossRef]

40. Kalra, S.; Sood, S.K. Secure authentication scheme for IoT and cloud servers. *Pervasive Mob. Comput.* **2015**, *24*, 210–223. [CrossRef]

41. Herzog, J. A computational interpretation of Dolev–Yao adversaries. *Theor. Comput. Sci.* **2005**, *340*, 57–81. [CrossRef]

42. Adeyemi, I.R.; Razak, S.A.; Salleh, M. A Conceptual Model for Holistic Classification of Insider. *arXiv* **2017**, arXiv:1706.05402.

43. Kebande, V.R.; Bugeja, J.; Persson, J.A. Internet of threats introspection in dynamic intelligent virtual sensing. *arXiv* **2020**, arXiv:2006.11801.

44. Kasar, S.; Kshirsagar, M. Open Challenges in Smart Cities: Privacy and Security. In *Security and Privacy Applications for Smart City Development*; Springer: Cham, Switzerland, 2021; pp. 25–36.

45. Liang, W.; Ji, N. Privacy challenges of IoT-based blockchain: A systematic review. *Cluster Comput.* **2021**, 1–19. [CrossRef]

46. Khorashadizadeh, S.; Ikuesan, A.R.; Kebande, V.R. Generic 5g infrastructure for iot ecosystem. In Proceedings of the International Conference of Reliable Information and Communication Technology, Johor, Malaysia, 22–23 September 2019; pp. 451–462.

47. Theofanos, M. Is Usable Security an Oxymoron? *Computer* **2020**, *53*, 71–74. [CrossRef]

48. Craggs, B.; Rashid, A. Smart cyber-physical systems: Beyond usable security to security ergonomics by design. In Proceedings of the 2017 IEEE/ACM 3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS), Buenos Aires, Argentina, 21 May 2017; pp. 22–25.

49. Kebande, V.R.; Karie, N.M.; Ikuesan, R.A. Real-time monitoring as a supplementary security component of vigilantism in modern network environments. *Int. J. Inf. Technol.* **2021**, *13*, 5–17.

50. Mocnej, J.; Miškuf, M.; Papcun, P.; Zolotová, I. Impact of edge computing paradigm on energy consumption in IoT. *IFAC-PapersOnLine* **2018**, *51*, 162–167. [CrossRef]

51. Kiani, F. A survey on management frameworks and open challenges in IoT. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 9857026. [CrossRef]

52. Agbehadji, I.E.; Frimpong, S.O.; Millham, R.C.; Fong, S.J.; Jung, J.J. Intelligent energy optimization for advanced IoT analytics edge computing on wireless sensor networks. *Int. J. Distrib. Sens. Netw.* **2020**, *16*, 1550147720908772. [CrossRef]

53. Ning, Z.; Huang, J.; Wang, X.; Rodrigues, J.J.; Guo, L. Mobile edge computing-enabled Internet of vehicles: Toward energy-efficient scheduling. *IEEE Netw.* **2019**, *33*, 198–205. [CrossRef]

54. Sharma, V. An energy-efficient transaction model for the blockchain-enabled internet of vehicles (IoV). *IEEE Commun. Lett.* **2018**, *23*, 246–249. [CrossRef]

55. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]

56. Singh, S.; Hosen, A.S.; Yoon, B. Blockchain security attacks, challenges, and solutions for the future distributed iot network. *IEEE Access* **2021**, *9*, 13938–13959.

57. Magnani, A.; Calderoni, L.; Palmieri, P. Feather forking as a positive force: Incentivising green energy production in a blockchain-based smart grid. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, Munich, Germany, 15 June 2018; pp. 99–104.

58. Singh, R.; Tanwar, S.; Sharma, T.P. Utilization of blockchain for mitigating the distributed denial of service attacks. *Secur. Priv.* **2020**, *3*, e96. [CrossRef]