Location proof systems for smart internet of things

Zafar, Faheem; Khan, Abid; Anjum, Adeel; Maple, Carsten; Shah, Munam Ali

Published in:
Electronics (Switzerland)

DOI:
10.3390/electronics9111776

Publication date:
2020

Citation for published version (APA):
Zafar, F., Khan, A., Anjum, A., Maple, C., & Shah, M. A. (2020). Location proof systems for smart internet of things: Requirements, taxonomy, and comparative analysis. *Electronics (Switzerland)*, *9*(11), [1776]. https://doi.org/10.3390/electronics9111776

electronics

MDPI

Review

Location Proof Systems for Smart Internet of Things: Requirements, Taxonomy, and Comparative Analysis

Faheem Zafar [1], Abid Khan [2], Adeel Anjum [1], Carsten Maple [3,*] and Munam Ali Shah [1]

[1] Department of Computer Science, COMSATS University Islamabad (CUI), Islamabad 42000, Pakistan; faheemiiui@gmail.com (F.Z.); adeel.anjum@comsats.edu.pk (A.A.); mshah@comsats.edu.pk (M.A.S.)
[2] Department of Computer Science, Aberystwyth University, Aberystwyth SY23 3DB, Wales, UK; abk15@aber.ac.uk
[3] WMG, University of Warwick, Coventry CV4 7AL, UK
* Correspondence: CM@warwick.ac.uk

Received: 12 July 2020; Accepted: 13 October 2020; Published: 26 October 2020

Abstract: In the current hyper-connected, data-driven era, smart devices are providing access to geolocation information, enabling a paradigm shift in diverse domains. Location proof systems utilize smart devices to provide witnessed proof of location to enable secure location-based services (LBS). Applications of location proof systems include safety, asset management and operations monitoring in health care, supply chain tracking, and Internet-of-Things (IoT)-based location intelligence in businesses. In this paper, we investigate the state of the art in location proof systems, examining design challenges and implementation considerations for application in the real world. To frame the analysis, we have developed a taxonomy of location proof systems and performed a comparative analysis over the common attributes, highlighting their strength and weaknesses. Furthermore, we have identified future trends for this increasingly important area of investigation and development.

Keywords: location-based services (LBS); location proof; location provenance; localization; blockchain

1. Introduction

Location-based services (LBS) rely on user geolocation, typically sourced through smart devices, to enable a wide range of services such as route guidance using Google maps, location-based social networks (LBSN), locator services (nearest restaurants, stores, and ATM, etc.), and location-based content delivery (games, news, and weather updates, etc.). However, incentive-based LBS (e.g., Foursquare offers badges and mayorships, etc. as venue-dependent rewards [1], the Bank of America gives location-activity tracking devices to employees and rewards them to improve productivity and reduce insurance cost [2]) can motivate users to provide false information regarding their location. For this reason, and others such as reliability and poor or compromised performance of devices, self-reported geolocation of user cannot be trusted without reservation. As such, it is important—and challenging—to prove a user's physical presence at a specific location at a specific time with a secure, reliable, and resilient process. The COVID-19 pandemic has disrupted the life and living pattern of everyone on this planet. To curb the spread of COVID-19 several contact tracing mobile applications have been developed [3]. However, this may result in disclosure of sensitive location data to unintended users. Although some of the applications do promise not to disclose this sensitive information, lack of trust has hampered the adoption of these applications in many countries. One such example is the application developed by federal Australian government, which claimed that they don't collect user's location data from the mobile but rather use Bluetooth technology to sense whether users who have opted in have come within nine meters of one another. Location proof

systems (LPS) provide a means for creating and sharing digitally signed meta-data that certify that a user was physically present at the claimed location at time instance [4,5]. In such systems, the proof of a user's location is generated in a secure manner, and an LBS can validate the proof through the LPS, and then provide the services requested. Beyond LBS, location proof systems are playing an increasingly significant role in health care applications (safety, asset management, and operations monitoring) [6,7], vehicular ad hoc networks (VANETS) [8], smart parking systems [9], Internet-of-Things (IoT) [10,11] and supply chain management [12]. Location proof systems can provide the proof for a number of locations use cases, such as a single location, travel path history (location provenance) and activity summaries (walking and running).

Localization [13] is a core concept driving the operation of location proof systems. Localization is a mechanism by which smart devices can report their location by computing their position relative to a cellular tower, satellite or other co-located devices. In location proof systems, localization is conducted utilizing physical hardware devices (including infrared [14], Wi-Fi infrastructure [15], Bluetooth [16] and GPS [17]) and algorithms (for example cellular tower triangulation, mobile device triangulation [18], audio-based positioning [14], IP address tracking [18], distance bounding protocols [19] and proximity [13,20]) in a secure manner. From a design perspective, centralized architectures were used initially to provide the basis for location proof systems. Centralized architectures, however, have been seen to suffer from scalability and cost issues. Another factor that restricted wide-scale implementation of centralized location proof system was its inherent dependency on a trusted third party for validation of generation of location proofs. These limitations have led to the advent of distributed location proof systems, beginning with the 2-party protocol (prover, location authority) [21]. On each site, a location authority is deployed to assist the prover in location proof generation. Later, the LBS validates the prover's presented location proof from the same location authority. However, these 2-party protocols can suffer when subjected to collusion attacks. To mitigate these collusion attacks, witness-oriented location proof protocols have been devised. These witness-oriented location proof systems may be 3-party (prover, location authority, witness) [22] or multi-party (prover, location authority (optional), multiple-witnesses) [15]. Recent research in location proof systems is heading towards exploring the application of blockchain technologies for decentralized location proof systems [23–27]. Distributed ledger technologies (DLTs), such as blockchain, are inherently useful for providing the location provenance in location proof systems, given their distributed nature. However, DLT-based location proof systems remain prone to collusion attacks. Some of the approaches employed to mitigate collusion attacks include outlier detection techniques [16] and entropy-based trust models, along with localization using the distance-bound protocol [15]. To the best of our knowledge, 3-way collusion (prover, location authority, witness—all participants of the location proof protocol are malicious at the same time) has not been mitigated by any scheme yet. In this paper, our primary focus will be on distributed location proof systems to address this challenge.

Our Contribution*:* The key contributions of this paper are:

1. Development of a taxonomy based on different aspects of location proof systems through a framework that considered nature (reactive or proactive), localization technique employed, deployment model, lifespan (one-time use, persistent), scope (single location proof or travel path history, and so forth), and primitives used for providing location privacy.
2. Discussion of the design challenges of location proof systems.
3. Providing a comparative analysis of distributed location proof systems, and providing insight into their capabilities.
4. Summarization of the possible attacks on location proof systems.
5. Identification of the future trends for research in the context of location proof systems (such as the application of blockchain models for location provenance and location-based access control).

Organization of Paper: This rest of the paper is organized as follows: In Section 2 we describe some of the prominent applications of location proof systems. In Section 3 a detailed discussion on trust evaluation and core requirements of location proof systems is provided. In Section 4 we discuss the evolution of location proof systems over the last few years. A detailed taxonomy of state-of-the-

art location proof systems is presented in Section 5, and a comparative analysis provided in Section 6. A detailed discussion on design challenges and future trends is provided in Section 7. Finally, the conclusion of the paper is provided in Section 8.

2. Application Areas of Location Proof Systems

The trustworthiness of location-proof systems demands that any system is cheat-proof [28]. Since a user is in full control of their own smart device, and potentially other local systems (such as a GPS-spoofing device), the possibility of cheating or colluding with other participants of the protocol to generate fake proof exists. Achieving trustable proof of physical user presence at a location using smart devices can play a vital role in combatting such attacks. To understand the need for location proof systems in practical scenarios, we discuss several candidate applications:

- Location-Based Data Restricted Access [29]: For outsourced data in cloud storage, the user may be restricted by their cloud storage service provider (CSP) through service level agreements (SLAs) to accessing data within restrict geographic region. Data access can be restricted at the granularity of city, state, time zone, or political boundaries. Therefore, users accessing the data are required to ensure the CSP about their geolocation. Location proof system can help both users and CSPs regarding compliance with SLAs.
- Student Attendance-Based Reward System: Today, smart devices are cheap enough to be afforded by students. To improve students' attendance in classes, universities can compel students to provide location proofs to ensure their physical presence in the classes using their smart devices. Students can then submit these proofs at the end of the semester to the teacher. Such attested attendance can be used in formative or summative assessment.
- Customer-Loyalty Reward System: In amusement parks, utility stores, café shops, etc., visitors may be offered special discounts based on proof of location, to provide, for example, evidence of the frequency of visits.
- Field Operations Monitoring: In certain situations, and countries, mobile operators delegate their post-paid customer's bill delivery to third party courier services. These courier service companies have field workers that delivering the bills to customers. If they fail to deliver bills to customers in a timely manner, a mobile operator can face complaints and less of customers. Therefore, both the mobile company and courier service can make their field operations more reliable through the use of location proof systems, enforcing their employees to obtain location proofs to ensure that they have delivered the bills to the customer's location. This can provide protection against false client claims (for example, they did not receive the bill or received it late). Similarly, pharmaceutical companies can utilize location proofs of the medical representatives and sales representatives to ensure that they are visiting hospitals and doctors.
- Location-Specific Team-Biased Audio Commentary of Sports [5]: Team-biased audio commentaries of a match can be produced and served based on the location of the user.
- Prevention against Stolen ATM Cards [30]: During a cash withdrawal from an ATM, it is possible to seek a match in the location of a customer's smart device and the ATM before allowing a transaction. Such a system might enable an alert to be raised if there is not a match in locations, and this used to identify stolen ATM cards, thereby preventing financial loss.
- Supervising People of Limited Personal Freedom: Another application of the location proof system is monitoring people who have been given bail by the court, but who are not allowed to leave the city. Due to the current pandemic of COVID-19, LBS can be used by medical units or governments to monitor the location the infected patients who in turn can use such system to show that they were present at the specified location at a specific time using the location proof system.

3. Evolution Timeline of Location Proof Systems

Based on an extensive literature survey, we have identified trends in location proof systems over the recent years. An evolution timeline has been provided in the Figure 1. Interest in this area started

in the 1990s when the importance of location information was realized, and research focused on methods to obtain reliable location information. The localization concept was introduced, in which a smart device was expected to convey its location with respect to another device, namely, a satellite, cellular tower or Wi-Fi access point. As techniques and technology progressed, location-aware schemes were designed using software-based or hardware-based localization techniques. Gabber et al. [31] proposed a mechanism incorporating multiple channels (GPS, cellular telephony, caller ID, satellites, etc.) to monitor the movement and location of smart devices. However, it was proved later that as malicious entities could bypass such multi-channel combination approaches [21], GPS signatures [32] and such approaches were prone to spoofing attacks [33]. Zugenmaier et al. [34] introduced the concept of location stamps, utilizing cell phones. Gruteser et al. in [35] highlighted privacy concerns and proposed an anonymity-based privacy preserving localization technique.

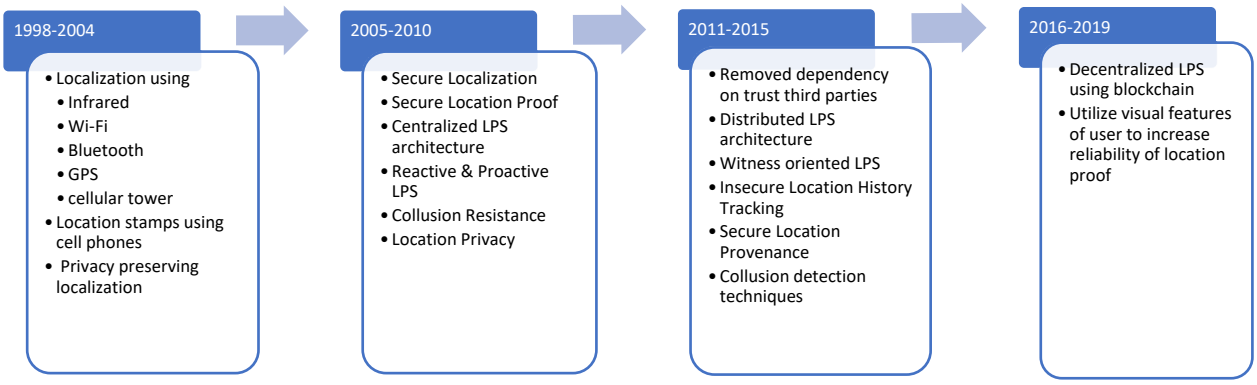

Figure 1. Evolution timeline of location proof systems.

However, with the introduction of incentives in LBS, the probability of cheating by the user with respect to their location information has led the research towards security aspects of localization techniques. Bauer et al. [36] discussed the vulnerabilities of wireless-based localization approaches against non-cryptographic attacks using a low-cost antenna. Their scheme was based on middleware to adjust the location information along spatial and temporal dimensions for a centralized location broker service. Techniques including measuring signal attenuation [33], measurement of the round-trip time (RTT) [19] and voice signatures [37] were unable to provide secure localization under adversarial settings. In [33], secure positioning of wireless devices under adversarial settings was discussed for the first time. Analyses of positioning algorithms (including received signal strength (RSS)), ultrasound time-of-flight (TOF), radio TOF, and civilian GPS) against position and distance spoofing attacks were performed, providing details regarding vulnerabilities. Signal attenuation techniques suffered from channel noise, and the constraint of line-of-sight makes them difficult in practical scenarios [22].

Saroiu et al. [5] devised a Wi-Fi-based protocol where Wi-Fi access points (AP) aid the prover for the generation of trusted location proofs. However, their scheme was prone to collusion attacks, as the AP and prover were able to collude, generating fake location proofs. User privacy was the primary concern in [5], as the real identity of the user was exposed to APs. The authors describe the security properties of secure location proofs and discuss the applications where LBS with incentives provide a motivation for users to lie about the location [5]. Later on, Saroiu et al. [38] used a trusted hardware trusted platform module (TPM) and virtual machine-based attestation to provide trust in the sensor readings. Gilbert et al. [39] proposed a TPM-based trustworthy mobile sensing platform to provide data integrity and privacy protection. Luo et al. [20] gave six design goals for a proactive (application agnostic) location proof system providing privacy protection. VeriPlace [40] provides a privacy-preserving location proof system with collusion resistance support. However, the assumption of a short interval between location proofs for collusion detection makes the system vulnerable. If the interval between two chronologically close location proofs was not close enough,

then the system treated them suspicious. Hence, the scheme puts a burden on the user to have frequent location proofs. All these schemes have no discussion over the chronological order of proofs.

Hassan et al. [41] designed a scheme for location proofs with wireless access points as location authorities and co-located smart devices designated as witnesses for proofs endorsement through Bluetooth, hence removing the dependency on the trusted third parties. Nonetheless, location provenance was maintained to record the chronological order of location proofs [41], which was missing in previous schemes. All the above schemes are under the category of centralized architectures. To remove the shortcomings of centralized models, research shifted to distributed models. Davis et al. [42] devised a scheme to generate location proofs with the help of smart devices within proximity. However, this scheme was not collusion resistant. APPLAUS [16] was designed for allowing interaction between co-located Bluetooth devices to mutually generate the location proofs. Pseudonyms were utilized to provide privacy protection by a central authority. The weakness of the scheme [16] was that high storage and communication overhead incurred due to dummy proofs generated periodically to preserve privacy. So-called betweenness ranking and correlation clustering approaches were used for collusion detection, which was power inefficient, and successful detection ratios >0.9 were possible only when the collusion percentage was <0.1. Ananthanarayanan et al. [43] introduced the so-called StarTrack framework, enabling tracks of information holding data about a person's location, time and metadata. The Tracks concept was quite similar to location provenance chains as data recorded in the time-ordered sequence. Besides, no security measures were taken, leaving the scheme vulnerable to malicious user manipulations. Gonzalez-Tablas et al. presented the notion of path stamps [44], extending the concept of location stamps [34] by recording the history of the visited location's proofs in a hash chain. However, none of the schemes formally described the requirements for a secure location provenance mechanism. OTIT [45] formally defined the requirements of the secure location provenance and performed a comparative analysis of different techniques used to maintain a provenance chain. These techniques include hash chain, block hash chain, bloom filters, shadow hash chain, multi-link hash chain, and RSA chaining. Comparison of these techniques is carried out from the perspective of provenance generation time, sequential verification time, sparse verification time, and space requirement. Brambilla et al. [23] proposed a first decentralized location proof system using blockchain for peer-to-peer overlay schemes. More recently, multiple blockchain-based location proof systems have been proposed [24,25]. Bucher et al. [46] proposed a secure and tamper-resistant location proof system based on visual features and image recognition provision without over-burdening the user.

4. Trust Evaluation and Requirements of the Location Provenance Chain

4.1. Trust Evaluation Criteria

Since most of the existing schemes provide a probabilistic guarantee for the prevention of collusion during protocol execution, we must rely on location provenance data analysis for post-collusion detection using the following criteria [40]:

1 Spatio-Temporal Correlation: Time difference and the distance between two consecutive location proofs can aid in the determination of false proofs. Consider a case where a user is able to successfully obtain location proof *LP1* for location *A* at time instance T_A and *LP2* for location *B* at time instance T_B. Now ($T_B - T_A$) is short enough that it is practically impossible for the user to travel from *A* to *B* in this significantly short time.

2 Trends Analysis: In trends analysis, the focus is on identifying the outliers where a user's location proof time deviates from past patterns since all past location proofs are part of the provenance chain. Data can be extracted from the provenance chain, and outlier detection techniques based on machine learning can be applied to detect where user location proofs deviate from the past pattern.

4.2. Evaluation Criteria for Protocol Characteristics

The following are the common parameters used for the evaluation of LPS [15,16,22]:

1 Proof Generation Time: Proof generation time is defined as the interval between the request generated by the user and the final proof generated by the system. It should be short enough (few seconds) for the system to be practically usable in real-time situations.
2 Decentralized Decision Time: This is the time interval between the participant approval request by the user and the final approval message received by containing the selected location authority and witness to aid them in proof generation.
3 Decision Block Size: The decision block size depends on the signature scheme used to provide non-repudiation by all entities involved in the decentralized decision. The size of the decision block will have a direct impact on overall storage capacity required by nodes in the administration layer.
4 Location Proof Size: Since location proofs will be stored on the user's mobile device, its size must be appropriate with respect to the storage capacity of smart devices.
5 Verification Time: It should be short enough (realistically a few seconds for most use cases) for the system to be practically usable.
6 Collusion Detection Rate: Given the potential for users to collude, is it important for a system to identify any cases of collusions. This can be ascertained through the use of simulated attacks.
7 Vulnerability Matrix: A vulnerability matrix can be generated to mark the scenarios where the system was able to resist the attacks and to determine the gaps where false proof generation is possible.

4.3. Requirements

The following are the requirements, as identified in [45,47], which must be satisfied by a location proof system:

1 Chronological Order: Order of the location proofs recorded in the provenance chain must match the sequence of locations visited by the user.
2 Time-Stamping: In a distributed environment, clocks of each of the entities in the location proof system can be different. Since the clock of the user's smart device cannot be trusted, time-stamping presents a real challenge for accurately recording the chronological order of location proofs of user visits.
3 Tamper Evidence: The location provenance chain should be tamper evident. If any tampering has been made to the chain or an individual proof, it should be detectable.
4 Validation: The provenance chain can be used to validate the location visit claims along with their chronological order.
5 Non-Repudiation: In the scenario of repudiation of a location visit by the user, the location provenance chain must be able to provide a user's signed location proof.

5. Taxonomy of Location Proof Systems

We present the taxonomy of location proof systems in Figure 2 based on following attributes: nature (reactive or proactive), localization techniques, deployment model, lifespan (one-time use, persistent), scope (single location proof or travel path history, etc.), and primitives used for providing location privacy.

- Nature: Location proof systems can be reactive or proactive [15,18,22,32]. Reactive proofs are application dependent, requiring dedicated hardware, and they cannot be re-used for other applications. In contrast, proactive proofs are application agnostic and are reusable for multiple applications. Proactive location proofs are tied to the user, whereas reactive location proofs are tied to the application.
- Deployment Model: For the deployment perspective, initially, secure location proofs systems relied on a centralized server [21,40,47]. Subsequently, due to performance issues, deployment

complexity, and dependency on trust third parties, focus has shifted to distributed models. Distributed location proof systems mitigate performance bottlenecks by eliminating the single centralized server and eradicate the need for trusted third parties [22,41]. Distributed location proof systems can be categorized into 2-party (prover, location authority (LA)) and witness-oriented protocols. Furthermore, witness-oriented location proof systems are subcategorized into 3-party (prover, LA, witness) and multi-party (prover, LA, multiple witnesses). However, the latest research is exploring a decentralized model of blockchain for location proof systems [23,24].

- Localization Technique: For location identification of the user's device, localization and network/localization infrastructure-independent approaches have been employed [47]. Localization is a mechanism by which a device provides location relative to some other device, maps, or satellite, etc. For localization, multiple software-based or hardware-based techniques have been used, including:
    - Fingerprint [48]: The fingerprinting technique relies on the variations of characteristics of signals. Received signal strength (RSS) is the most used method for fingerprint-based localization. Beyond measuring the difference between signals in various positions, two other approaches commonly used include radio-map based fingerprint localization and map-free fingerprint localization. Techniques based on a radio map first establish a map of location points and signal strengths. Later on, to identify the location of the device, the pre-collected signal strengths against saving points are used as a reference, however, this technique is not reliable for secure localization. On the other hand, map-free fingerprint localization reduces the complexity of the radio map technique, but it is only applicable for non-static localization.
    - Distance-Bounding Protocols [4,15,19,49]: A distance-bounding protocol is a technique that allows the verifying party to attain an upper bound on the distance of the target. It works on single-bit challenge requiring a rapid single-bit response. Multiple rounds of this challenge response are performed, and delays of response are analyzed to determine the upper bound on distance. A distance-bounding protocol work by measuring round-trip time (RTT) or signal strength. However, physical presence detection using distance-bounding protocols involves a trade-off between performance and localization reliability.
    - Context-Based Modalities [50]: The underlying idea for context-based localization techniques is the measurement of contextual values (such as acoustic environment, ambient light and noise level, atmospheric gases, temperature, humidity and air pressure, Wi-Fi and Bluetooth signal strength) and the utilization of them as a proof of physical presence at the location. The verifier and user simultaneously capture such contextual data. Then, the user generates the proof of presence, including the contextual information, and the verifier validates the contextual measures to certify the physical presence of the user.
    - Proximity [4,13,20]: Proximity localization focuses on the fact that the user is within a certain range of known access points, enabling the estimation of its approximate location. It is normally used for localization in link-based or connection-based wireless communication.
    - Triangulation [14,48]: In triangulation, geometric mathematics are involved in calculating the user's location. Triangulation can be angle based, time based, or RSS based. Angle-based triangulation measures the angle of the received signal and is dependent on directional antenna technology. In time-based triangulation, the travel speed of wireless signals serves as a reference, and the time difference is measured for communication between the beacon and the user's device to determine the approximate location of the user. For time-based triangulation, two methods are commonly used: (i) time-of-arrival (ToA) and (ii) time-difference-of-arrival (TDoA). ToA measures the time difference of the packet's transmission between the beacon and smart device. TDoA extends ToA by synchronizing the beacon's time and evaluating their hyperbolic curves for potential locations. The intersection point of these curves is supposed to be a correction transmission, which is used to estimate the

user's location. In RSS-based triangulation, the received signal strength is used to infer the user's location.

- Beaconing [51]: In the beaconing approach, a location verifier beacons the specific information, and users in the vicinity are required to capture this information utilizing the built-in sensors of the smart device, e.g., Wi-Fi or Bluetooth.
- Mobile Network Operator/Cellular Tower-Based Approach: Two types of approaches are discussed in the literature: (i) smart devices themselves calculate their position with the help of a base station [52], and (ii) a mobile network operator calculates the position of the smart device [30].

- Lifespan: Based on the lifespan of location proofs, they can be categorized into persistent and non-persistent types. Non-persistent location proofs [30,53] are one-time use only, e.g., to ensure that the cash withdrawal at an ATM is by the cardholder him/herself—the location of the smart device of user and ATM should be same. On the other hand, persistent location proofs are stored in permanent storage such as in a user's mobile device [22], centralized server [41] or on a blockchain [23]. Persistent location proofs could be reused in the future to prove the claims of presence at a location at a time instance. For example, at the end of a semester, students can present the location proofs of attendance in classes to the teacher. Similarly, an engineer can present location proofs of his site visits at the end of the month.
- Scope: Location proof systems can support single location proof [4,15,16,18,41] activity summaries, distance covered, or travel history established by recording the chronological order of single location proofs in a chain [22,23,45]. Activity summaries [2,54] represent the user's physical activity, such as jogging on a track covering a certain distance. Systems supporting activity summaries can rely on existing infrastructures like social network operators. Infrastructure-independent and hybrid schemes for generating activity summaries also exist in the literature.
- Location Privacy: Location privacy is an important aspect of location proof systems. It determines the granularity level of the location information to be exposed to the auditor. To preserve location privacy, cryptographic and non-cryptographic techniques are both used in existing schemes. Cryptographic [4,15,22,41,55,56] techniques include hashing, MACs, symmetric encryption, and digital signatures. Non-cryptographic [47,57] techniques can use the channel's physical layer characteristics to generate signatures.

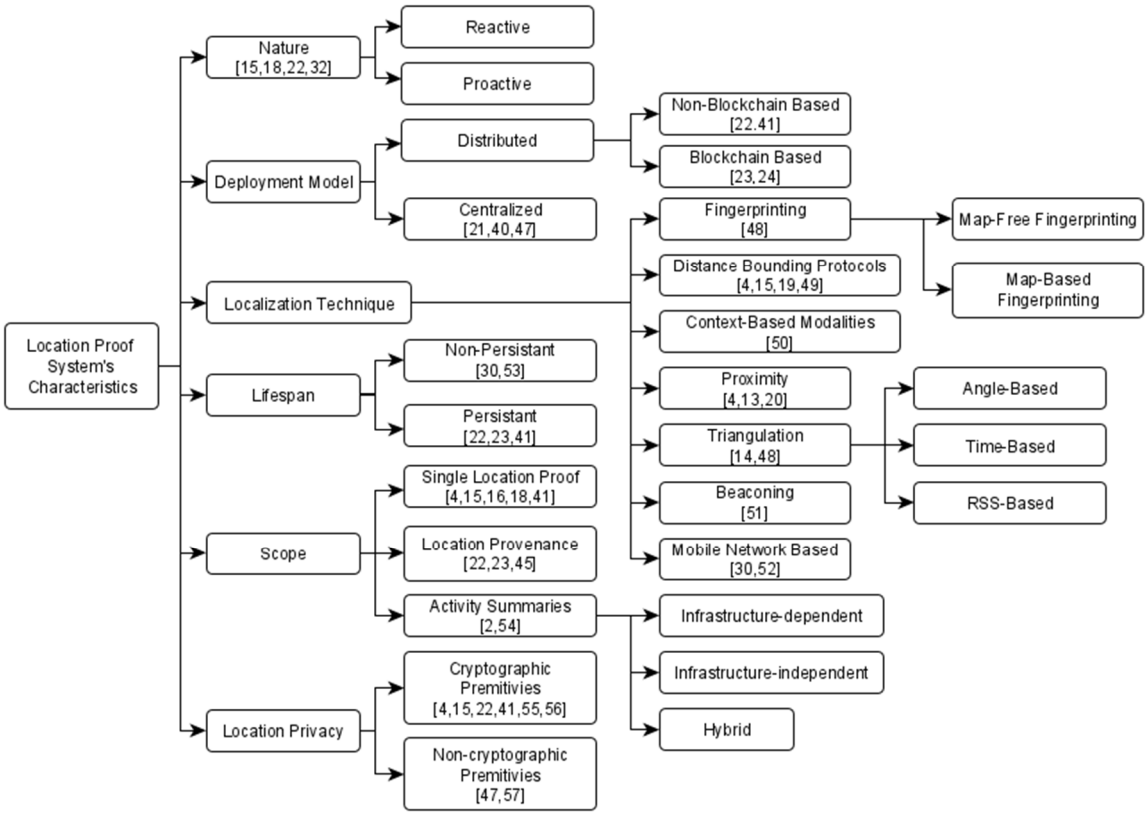

Figure 2. Taxonomy of location proof systems.

6. Comparative Analysis of Location Proof Systems

To study the comparative advantages of location proof schemes over one another, we have selected five attributes including the localization method, cryptographic primitives used, privacy preservation capability, participants trust evaluation, attacker model from a security perspective and in general strengths and weaknesses of the schemes. Table 1 summarizes the schemes regarding the above-mentioned attributes. As the primary focus of this paper is on a distributed location proof system and persistent location proofs, most of the schemes selected for comparison fall in this category. To maintain a consistency and not to overburden the reader, we have organized this section based on the cryptographic technique used by the scheme.

Location Proof Systems Based on Asymmetric Cryptographic Primitives: Gambs et al. [4] designed a privacy-preserving location proof system PROPS. Instead of relying on a trusted third party for location claim verification, PROPS allowed the users to generate proof of physical presence on a location in collaboration with its neighbors. Salient characteristics of the proposed scheme are unforgeability and non-transferability of location proofs with protection against localization attacks. The authors introduce the notion of location proof share, a time-stamped digital signature generated by a neighbor for the location of the user. Multiple location proof shares combine up to make an LP, which provides granularity level of location information of the user to preserve their privacy against the verifier. Further, the Anonymity Lifter (AL) is a trusted third party that can disclose the anonymity of user on a needs basis (for example on the request of the judge). The scheme assumes the prover, witness, and verifier as untrusted and evaluates the *security* against collusion attacks (like P-P collusion, terrorist fraud attack, and worm-hole attack, etc.). The scheme utilizes cryptographic primitives such as CL signatures, commitment schemes, and zero-knowledge proofs. Wang et al. [15] have proposed STAMP, a spatial-temporal provenance assurance with the mutual proofs scheme. STAMP ensures user's privacy while providing the integrity and non-transferability of location proofs. To guard against collusion attacks, the entropy-based trust model is utilized. It reduced the dependency on multiple trusted parties to a single semi-trusted party, i.e., certification authority (CA). The scheme

also supports the granularity level control for exposure of location information to the verifier by the user. The authors are the first to deal with two collusion attacks: (i) P-P collusion: user A physically present on target location generates a false proof for B by masquerading; (ii) terrorist fraud attack: two malicious users collude to generate fake proof of location for each other. To prevent terrorist fraud attacks, the Bussard–Bagga distance bounding protocol is used with a recognized trade-off in performance.

Hasan et al. [41] introduced their first witness-oriented distributed location proof system with secure location provenance with the assumption of untrusted location authority. Location provenance provides a verifiable claim of travel path in a secure manner by keeping the chronological order of individual location proofs. In the proposed scheme, two location provenance tracking mechanisms were devised, one using a hash chain and the other using bloom filters while preserving the location privacy. The authors identified the possible attacks on a location proof system, including false presence, false time, reordering, implication, false endorsement, denial of presence, proof switching, and doppelganger. From a security perspective, the scheme enumerated the adversaries and classified the possible attacks into two groups, i.e., single entity attacks and multiparty collusion attacks. The same authors extended the work in [41] to propose the WORAL [22], a distributed witness-oriented secure location provenance framework for mobile devices. WORAL is a complete working system built by integrating the asserted location proof (ALP) of [18] and the OTIT [45] model for managing secure provenance. In WORAL, collusion models and corresponding threats are well discussed, and it is claimed that the system is only 12.5% vulnerable due to 3-way collusion. For evaluation of the protocol, characteristics considered were proof generation time, maximum distance threshold (depending on localization technique), proof's size, number of participants of protocol, collusion detection rate, and vulnerability matrix to identify the scenarios where fake proof generation is possible. For privacy preservation, crypto-IDs are used such that the many-to-one relationship holds between crypto-ids and the real identity of the user.

Brambilla et al. [23] proposed a first decentralized location proof system using blockchain for peer-to-peer overlay schemes. However, participant selection control remains with the user, therefore, decentralization standalone still makes their scheme vulnerable to collusion attack. The proof generation protocol of the scheme allows the direct communication between the prover and responding peer in the P2P network of the blockchain, allowing participants to collude to generate false location proofs. The prover may not be physically present at the reported location, and the responding peer may assist in the generation of a false proof of location. After completion of the proof generation phase, the prover disconnects from the network and may become unreachable. Before committing the proof on the blockchain, for validation of the proof generated by the prover and the responding peer, the scheme has the assumption that at least one of the participant peers (either the prover or responding peer) must remain reachable by other co-located peers in a network with short-range communication technology. Since the responding peer is part of the network and is reachable by co-located peers in the network, the prover will be able to cheat the system due to collusion with responding peer. Indeed, their scheme has a strong assumption that all available neighbor peers are not colluding, but they are deceived in the above scenario, as the responding peer appears present at the reported location. However, the author's scheme is resistant to backdating and future-dating attacks.

Pham et al. [2] proposed one of the first cheat-resistant methods, a privacy-preserving location proof system for user's activity summaries utilizing the existing infrastructure deployed in urban areas. These activity summaries are utilized by companies to offer rewards to their employees who, in return, achieve better productivity and lowest health insurance cost. The scheme proposed by the authors is infrastructure dependent; location proofs are collected during activity through centrally operated Wi-Fi access points. A service provider utilizes these intermediate location proofs of complete activity and produces a final activity summary proof for the user. Pseudonyms are used for location privacy preservation. The authors applied cryptographic techniques and geometric algorithms on real datasets obtained from FON community networks and Garmin Connect activity-based social networks for evaluation and achieved an accuracy of 76% for the lower bounds of the

distance covered. The Google Elevation API is utilized to generate elevation/distance proof. The delay-based challenge response mechanism is applied to prevent proxy-relay attacks. However, the proposed system's security is limited and it is unable to resist Wi-Fi channel characteristics-based attacks, such as a user increasing the transmission power of their device to show falsely that they are close enough to the access point. The scheme presented in [2] provides no protection against attacks launched by collusion of a social network operator and an access point network operator. However, the delay-based challenge response mechanism is applied to prevent proxy-relay attacks. Again, pseudonyms are used for location privacy preservation. The *secure-run* scheme [54], an extension of [2], has been proposed with a focus on improving the accuracy of activity summaries. Along with accuracy, user privacy is the primary concern as a service provider is untrusted. However, from a security perspective, the scheme is also vulnerable to collusion attacks when a user, service provider and access point maliciously collude to generate a fake activity summary.

Camenisch et al. [30], instead of relying on the phone's self-computed location, devised a mechanism that prefers to rely on a user's location provided by the mobile network operator (MNO). In this scheme, the service provider depends entirely on the MNO to ensure that the user him/herself is physically present at the reported location. However, protection of the privacy of the user's location from the service provider is required. For privacy preservation, [30] introduced the concept of the reported area as the user's location and reference area, where the user is expected to be by the service provider. Location evidence binds the reported area with phone identifier, which in turn is bonded with the user's identity. Anonymous credentials are used to make the service provider verify that the user is present within the expected area instead of the exact user's location. Furthermore, anonymous credentials resist the tampering, replay, and collusion attacks for achieving reliable location proofs.

Subhashri et al. [58] designed a location proof scheme utilizing ciphertext policy attribute-based encryption (CP-ABE) for collusion detection and the blowfish algorithm for secure location proof sharing. Multiple witnesses could be involved to make the collusion difficult. However, their scheme provides very limited collusion resistance. The scheme has no support to track the travel history, preserving the chronological order of location proofs.

Table 1. Comparative analysis of location proofs system. Abbreviations: entities' trust evaluation (ETE), location privacy (LP).

Reference	Localization Via	Cryptographic Primitives	LP	ETE	Attacker Modal	Strength	Weakness
[2]	Wi-Fi	Public-key encryption scheme	✓	×	The prover is untrusted, while the social network operator and Wi-Fi access point network operator is semi-trusted (honest-but-curious).	The accuracy of lower bounds of distance covered is achieved where multiple access points co-exist. The delay-based challenge response mechanism is applied to prevent proxy-relay attacks. Pseudonyms are used for location privacy preservation.	Unable to resist Wi-Fi channel characteristic-based attacks like if the user increases the transmission power of his device to falsely show that he is close enough to the access point. No protection against attacks launched by collusion of the social network operator and the access point network operator.
[4]	Proximity testing using the Bussard–Bagga distance bounding protocol	Unique group signature, Pederson commitment, zero-knowledge proof, hashing	✓	×	Prover, witness, and verifier are untrusted. CA and AL are trusted.	Group signatures used to preserve the privacy of users, and original identity can still be disclosed by LA. For granularity levels of location information, hash chaining is used.	Higher memory usage. Unable to resist P-W collusion attacks.
[15]	Bluetooth, Wi-Fi	DSA, RSA, SHA-1, 128-bit AES	✓	✓	Prover, witness, and verifier are untrusted. CA is semi-trusted.	Tamper-evident location proofs. Witness assertion support provides protection against 2-way collusion. Multiple witnesses can be involved in proof generation. Entropy-based trust modal for collusion detection. Granularity level supported for exposing location information.	To testify, user proximity relies on the Bussard–Bagga distance bounding protocol, which is time-consuming. Prover-witness collusion detection efficiency is higher when the user's mobility is high and lower when mobility is lower. Location provenance for tracking travel history is not supported.
[22]	Wi-Fi	RSA (2048-bit) signatures, SHA-2 hashing with digest size 256 and 512 for hashing messages in protocol	✓	×	Prover, location authority and witness are untrusted.	Tamper-evident, verifiable location proofs. Location provenance supported for capturing the travel history with chronological order preservation.	Unable to resist 3-way collusion. The auditor can be overloaded by a malicious user and therefore vulnerable to the single point of failure.
[23]	Bluetooth	ECDSA	✓	×	All participants are part of a peer-to-peer network and can be in one of three roles (prover, request	Decentralized location proof system. Distributed consensus used to save location provenance over the blockchain.	No support for witness assertion. No protection against prover and request receiving a peer collusion attack.

					responder and verifier) at the instance of time. All are assumed malicious but not all same instance.		No protection against 3-way collusion.
[30]	Mobile network operator (MNO)	Anonymous credentials	✓	×	MNO is a trusted location source, however, the service provider is semi-trusted, and the prover is untrusted.	Privacy-by-design approach is used by utilizing anonymous credentials. No dependency on sensors in mobile devices. Location information is trustworthy even if the mobile device is fully compromised. The scheme is able to resist replay attacks, MNO and service provider collusion attacks.	Reported area accuracy is limited.
[41]	Wi-Fi, Bluetooth	1024-bit DSA-signatures, SHA-1 Hashing	✓	×	Prover, location authority and witness are untrusted.	Eliminated the dependency on multiple trusted parties. Hash chain- and bloom filter-based location provenance supported.	No protection against 3-way collusion and Sybil attacks.
[47]	Bluetooth	Non-cryptographic technique	×	✓	Prover and verifier both are malicious.	No reliance on network/localization infrastructure. The centralized architecture provides a global view of the complete system. Location claims are accepted and rejected on the basis of trust scores of neighbors.	Centralized location verification authority is a single point of failure as becomes the bottleneck. Limited collusion resistance. No protection against Sybil attacks. Prone to physical layer characteristic attacks such as using a non-standard wireless interface to generate higher signal strength. No location privacy protection mechanism.
[49]	Distance bounding protocol	anonymous credentials and the Camenisch–Lysyanskaya (CL) signature scheme	✓	×	The prover is untrusted, and the verifier is honest but curious. LNS is assumed trusted.	Verifiable multilateration is used for provable protection against spoofing attacks and supports location verification.	The location naming service (LNS) is a trusted store containing signed entries that map user-defined labels (referred to as location labels) to their corresponding sets of locations. DoS on LNS can downgrade the whole system.
[50]	Contextual variation measurement matching	-	✓	×	The prover is malicious, and the verifier is trusted.	Context-based proof of presence (PoP) with entropy measurement techniques to resist against malicious prover.	Vulnerable to relay attacks.

						PoP utilizes an ambient noise level for privacy protection instead of actual fine-grained audio signals.	
[51]	Wi-Fi signal characteristics, e.g., channel state information (CSI)	SHA-1 hashing, public key-signature scheme and fuzzy vault (a cryptographic primitive)	✓	×	The prover is dishonest, while the access point and verifier are honest and trusted.	Utilize wireless channel characteristics to validate user's location and context information Fuzzy vault used to preserve privacy. Better performance because the time of proof generation is independent of the size of the location tag embedded in location proof and the distance between a mobile user and the location proof provider. Experimental evaluation conducted for indoor environments.	No support for location provenance. Vulnerable to collusion attacks.
[53]	Wi-Fi	TLDC (two-layer differential coding), CFO encryption	✓	×	LBS provider is assumed trusted, and the user is untrusted.	Physical layer information (carrier frequency offset (CFO), multipath, channel state information (CSI)) available in legacy Wi-Fi preamble is used for user's location information verification.	Based on experimentation, authentication accuracy is 93.2%, while privacy leakage is 45.7% in comparison to state-of-art approaches. LBS provider and user collusion attack not considered.
[54]	Wi-Fi	The digital signature scheme, order-preserving encryption	✓	×	Prover and the service provider are untrusted. However, access points are semi-trusted.	Maximize the accuracy of summaries by computing an optimal set of access points to communicate with. Pseudonyms used for privacy preservation.	Limited location privacy protection against access point operators. Unable to resist prover, access point and service provider collusion attacks.
[55]	GPS, Bluetooth, Wi-Fi	Shamir secret sharing scheme, symmetric encryption, Diffie–Hellman protocol	✓	×	CA and verifier are semi-trusted, while prover and witness are untrusted.	Better performance in detection and resistance against prover–prover collusion and prover–witness collusion attacks. For privacy protection, pseudonyms are used.	The more witnesses, the more overhead encryption and decryption of key shares. Unable to resist 3-way collusion as witness selection control lies with the prover. Location provenance (to track the chronological order of proofs) is not supported. In the basic scheme, due to privacy protection, the Diffie–Hellman protocol used is not

							resistant to man-in-the-middle attacks.
[58]	Bluetooth, Wi-Fi	Ciphertext policy attribute-based encryption (CP-ABE) blowfish	✓	×	The prover is untrusted whereas, the witness can be trusted or untrusted.	Ciphertext policy attribute-based encryption (CP-ABE) is used to detect collusion. Multiple witnesses can be involved to make the collusion hard.	No support for location provenance. Limited collusion protection.
[59]	GPS	Prefix-verifiable MAC (PMAC)	✓	×	Location authenticator is assumed trusted, while prover and verifier are semi-honest	Prefix-verifiable MAC (PMAC) is used for tamper-proof location evidence. Reduced computation and communication cost. Granularity level for exposing location information.	No support for location provenance.
[60]	Bluetooth	Symmetric shared key and a public key signature scheme	✓	✓	Prover and witness both are assumed malicious.	Encounter-based location proof exchange. Mechanism-based on the concept of physical–social locations (PSL) or a witnessing zone, which is the geographic region that is frequently visited by people over a fairly long period with social significance, that is, workplaces or neighborhoods. Reputation model to Evaluate a user's behavior as a witness. MPSL is a lightweight, accurate and fast.	Prone to prover–witness collusion, however, the cost of launching such attach is higher because the prover has to generate multiple proofs for the same location. System's performance depends on the user's density and witnessing zone's coverage.

Der-Yeuan et al. [49] introduced a wide-area secure positioning system (W-SPS) to provide reliable location proofs in a privacy-preserving manner. The system features two main components: a (i) secure positioning infrastructure (SPI), responsible for providing verifiable location statements, and a (ii) location name service (LNS), which facilitates the users to map the locations to labels and the verification of location statements against mapped labels. SPI uses verifiable multilateration to provide provable protection resilience to spoofing attacks and supports location verification. A distance bounding protocol is used to ensure that the prover is within a certain range of the claimed location. To preserve a user's privacy, anonymous credentials and the Camenisch–Lysyanskaya (CL) signature scheme are used. Furthermore, the Fiat–Shamir heuristic is used in the verification phase to achieve zero-knowledge proof to preserve the user's privacy against any honest-but-curious verifier. Chitrali et al. [51] introduce a scheme that relies on a Wi-Fi signal characteristic. i.e., channel state information (CSI) of the physical layer. The location proof in this scheme is segregated into two features sets, thereby making any fake proof generation infeasible by an adversary that does not know both sets. Their scheme additionally incorporates the user's context information by utilizing Wi-Fi multipath information. The channel state information at the time of proof generation makes it hard for the user to forge location proof, i.e., a malicious user cannot transfer, tamper, or reuse the old valid proof. Another promising feature of their scheme is that performance is independent of the distance between the user and access point and requires no changes at the hardware level as required for distance bounding protocols. In [51], both the user and verifier are assumed untrusted.

Location Proof Systems Based on Symmetric Cryptographic Primitives: Haibu et al. [59] proposed a spatiotemporal integrity scheme using a prefix-verifiable message authentication code to achieve unforgeable location evidence on mobile devices. The threat model of the scheme assumes the user and the verifier both are semi-trusted. A promising feature of the scheme is support for spatiotemporal predicates. The method presented in [59] has a location authenticator module, which relies on the CPU security (e.g., ARM's TrustZone and Intel's trusted execution technology) to boot-load a trusted environment for providing enterprise-level security. Samsung KNOX is another example of providing a trusted environment in smart devices. The location authenticator on the user's mobile device ensures a secure localization. Ni et al. [60] introduced the encounter-based location proof mechanism by categorizing the locations as witness zones. Each witness zone is the geographic region that is frequently visited by people over a fairly long period, e.g., workplaces or neighborhoods. These frequent visitors of the specific zone may become witnesses. The prover will be required to generate multiple proofs for a predefined period-of-time with the help of these witnesses to prove physical presence at that location. However, the system's performance depends on the user's density and coverage of the witnessing zone. From a security perspective, the scheme can resist non-collusive attacks, but is unable to resist prover–witness collusion attacks. Bluetooth is utilized to mitigate the eavesdropping attack.

Location Proof Systems Based on Hybrid Cryptographic Primitives: Mengjun et al. [55] designed the location proof system with a focus on solving the shortcomings of STAMP [15] Their scheme claims to provide a higher level of privacy with better performance than [15], as distance-bounding protocols are time-consuming and therefore affect the performance of STAMP. From a collusion detection perspective, STAMP relies on long-term statistics and is applied to an entropy-based mechanism for the user's trust evaluation, and therefore is unable to detect collusion attacks in real-time. STAMP also has limited resistance to prover–prover and prover–witness collusion attacks, especially when users are not static. Shamir's secret sharing scheme is applied over prover's private key in the proof generation protocol of [55] to resist the collusion of a prover, as his private key will be disclosed to other participants. Furthermore, to preserve privacy against a verifier, the prover is supposed to communicate with the verifier using an anonymous channel such as TOR.

Location Proof Systems Based on Non-Cryptographic Primitives: Talasila et al. [47] proposed a location proof system that relies on a centralized location authority. The centralized location authority maintains historical data which contain (i) user's trust scores collected over a period (ii) and a list of verifiers with a verification count for each user. Historical data are used to prevent collusion attacks by a group of users or user–verifier pairs by analyzing the historical trust values and malicious

patterns. Furthermore, for location claim acceptance, spatiotemporal correlation (the time difference between the current and last location proof should be practically possible for physical movement between two locations) and the verifier's trust score are considered. Moreover, the authors' scheme does not provide location privacy protection and is prone to physical layer attacks such as using a non-standard wireless interface to generate a higher signal strength. Wei Wang et al. [53] devised the privacy-preserving location authentication mechanism named "PriLA" utilizing the Wi-Fi physical layer information. PriLA exploited detrimental features (carrier frequency offset (CFO), channel state information (CSI), multipath) of a wireless system to generate privacy-preserving signatures and verification of the user's physical location. Multipath profiles for the user are extracted using multiple antennas as they provide an environment's physical state, which is dynamic and hard to forge. PriLA captures similar multipaths from multiple users and compares them to authenticate user physical presence without any localization method. Experimentation showed that authentication accuracy is 93.2% while privacy leakage is 45.7% in comparison to state-of-art approaches. Miettinen et al. [50] proposed the concept of proof-of-presence (PoP) using context information (i.e., an acoustic environment, ambient light and noise level, atmospheric gases, temperature, humidity and air pressure, Wi-Fi and Bluetooth signal strength) for verification of the user's location claim. The primary focus of the scheme is to resist the context-guessing attacks. To achieve resilience against context-guessing attacks, authors relied on two approaches: (i) surprisal filtering, which works by estimating the entropy of contextual fluctuations, serving the purpose of PoP, and (ii) measuring the longitudinal observations of ambient modalities (like noise level and ambient light). The first technique reduces false positives; however, the false negative rate also increases. Meanwhile, by utilizing the audio and light modalities from built-in sensors of a smart device, the proposed scheme is better at mitigating context-guessing attacks in comparison to Wi-Fi- and Bluetooth-based approaches. However, while the scheme is still vulnerable to relay attacks, the practical cost of launching such attacks is very high.

7. Design Challenges and Future Research

For a reliable, secure, and efficient location proof system, the following dimensions have a primary impact:

- Proof Generation Time [22]: Proof generation time is the interval between the request generated by the user and the final proof generated by the system. It should be short enough (a few seconds) for the system to be practically usable. However, there is a trade-off between security and proof generation time. Higher security guarantees, with the higher proof generation times, make the system impractical in real scenarios.
- Storage [41]: This concerns where proofs are stored. Storing all proofs in a central server will result in bottlenecks. In the distributed model, each location may have common storage for location proofs; nevertheless, in the verification process, it becomes difficult to access the proofs from distributed locations. Storing the location proofs over the user's smart device is preferred if the user is trustable. However, the user has full control over their device and can manipulate the proofs, thus demanding proofs to be tamper evident.
- Proof Size [41]: Location proof size becomes a constraint for location proof systems keeping in view the storage capacity of smart devices and location authority, especially when location provenance is supported. Additionally, space requirements change when location privacy is enabled, supporting granularity levels for location information with respect to entities in the system.
- A Number of Entities/Witnesses Involved [15,22]: Distributed location proof systems and witness-oriented location protocols involve two or more entities in the proof protocol. A number of entities involved in the location proof protocol provide reliability of the physical presence of a user at a location. However, having more entities in the protocol provides reliability at the cost of proof generation time.
- Collusion Resistance [15,22]: When multiple entities are involved in the proof generation protocol, collusion attack possibility increases. Since all the entities are not trustable, the location

proof system must be collusion resistant. In this context, trust evaluation mechanisms can mitigate the collusion problem to some extent.

- Security: For trustworthiness of the location proof system, the following attributes must be provided:
- Integrity: Users should not be able to create a fake location proof alone or by collaboration with other entities [15,38].
- Non-Transferability: All provers should not be able to falsely claim ownership of any legitimate proof generated for any other prover in the system [15,38].
- Location Privacy: This determines the granularity level of location information that the user wants to share with auditors [38,41].

If the location proof system supports the location provenance, then the following properties must be satisfied:

- Chronological Order: Order of the location proofs recorded in the provenance chain must depict the same sequence as the locations visited by the user [15].
- Time stamping: In a distributed setup, clocks of the entities in the location proof system can be different, as the clock of the user's smart device cannot be trusted. Therefore, time stamping is a real challenge to accurately record the chronological order of location proofs of user visits [41].
- Tamper Evidence: A location provenance chain should be tampering evident. If any tampering has been done to the chain or individual proof, it is detectable [15].
- Validation: The provenance chain can be used to validate the location visit claims along with their chronological order [15].
- Non-Repudiation: In the scenario of repudiation of a location visit by the user, the location provenance chain must be able to provide proof of the user's presence [15].

Future of Location Proof Systems with Blockchain

Blockchain is a decentralized linked data structure implicitly providing features like tamper resistance, non-repudiation, and chronological order without any dependency on trusted third parties, making it ideal for location proof systems to provide location provenance. Blockchain is a cryptographically secure distributed ledger. The blocks containing the hash of the previous block establish the chain, providing the integrity of stored data and tamper resistance. A peer-to-peer network of nodes derives Blockchain operations, and the distributed consensus mechanism ensures that only valid blocks become part of a chain. Algorithms can be designed inspired by the distributed consensus of blockchain to allow for decentralized secure location proof systems. Already research has begun on blockchain-based location proofs [24,25,41]. In blockchain-based location proof systems, each block is verified to be valid before making it part of the blockchain. For example, Nosouhi et al. [10] proposed a blockchain-based secure location verification scheme. The authors' scheme has a verifier entity like the minors in Bitcoin, and this is responsible for validating the transaction: (1) the prover's signature matches its public key; (2) the witness's signature matches its ID; and (3) the bridge's signature is correct. Moreover, there is no negative acknowledgement regarding the transaction in the network. After all these validations, location proof is considered valid.

8. Conclusions

In this paper, we have highlighted the need of location proof systems, design challenges and requirements; we have developed the taxonomy using the identified attributes; and we have discussed dimensions of location proof systems with respect to their application in diverse domains. We have also provided a comparative analysis of schemes to give an insight into the technical aspects of location proof systems. To give the overview of the state-of-art technology, we have presented an evolution of location proof systems. The advent of smart devices has revolutionized the modern world, and because of this, information on the current physical location of a person has become of great significance. LBS with incentives motivate users to lie about their location. As such, it becomes

challenging to prove a user's physical presence at a specific location at a specific time instance in a secure manner. Smart devices have paved the way for location proofs. Location proof systems have evolved over time from the simplest form of localization to fully decentralized blockchain-based applications. In this regard, this paper has identified major challenges in the design of secure location proof systems, which must be considered by the future research in this domain. Blockchain-based approaches will dictate the future schemes because of the distributed nature of the design provided by this new technology.

Author Contributions: Conceptualization, F.Z., A.K. and A.A.; methodology, F.Z., A.K.; software, F.Z.; validation, M.A.S., F.Z. and A.K.; formal analysis, C.M.; investigation, A.A.; resources, C.M.; data curation, F.Z.; writing—original draft preparation, F.Z., A.K. and C.M.; writing—review and editing, F.Z., A.K., C.M. and M.A.S.; visualization, A.A. and A.K.; supervision, A.K. and A.A.; project administration, C.M. and A.K.; funding acquisition, C.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research and APC was funded by grants EP/R007195/1 (Academic Centre of Excellence in Cyber Security Research—University of Warwick); EP/N510129/1 (The Alan Turing Institute); EP/S035362/1 (PETRAS National Centre of Excellence for IoT Systems Cybersecurity); and EP/R026092/1 (FAIR-SPACE).

Acknowledgments: We would also like to add special thanks to Elixir Technologies Pakistan for all support in accomplishing the research work. Maple would like to acknowledge the support of EPSRC.

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

Reference

1. Carbunar, B.; Potharaju, R. You unlocked the mt. everest badge on foursquare! Countering location fraud in geosocial networks. In Proceedings of the 2012 IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2012), Las Vegas, NV, USA, 8–11 October 2012.
2. Pham, A.; Huguenin, K.; Bilogrevic, I.; Dacosta, I.; Hubaux, J.-P. Securerun: Cheat-proof and private summaries for location-based activities. *IEEE Trans. Mob. Comput.* **2016**, *15*, 2109–2123.
3. O'Neill, P.H.; Ryan-Mosley, T.; Johnson, B. A Flood of Coronavirus Apps Are Tracking Us. Now It's Time to Keep Track of Them. MIT Technol. Rev. Available online: https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/ (accessed on 15 September 2020).
4. Gambs, S.; Killijian, M.O.; Roy, M.; Traoré, M. PROPS: A privacy-preserving location proof system. In Proceedings of the Reliable Distributed Systems (SRDS), 2014 IEEE 33rd International Symposium on Reliable Distributed Systems, Nara, Japan, 6–9 October 2014.
5. Saroiu, S.; Wolman, A. Enabling New Mobile Applications with Location Proofs. In Proceedings of the 10th Workshop on Mobile Computing Systems and Applications, Santa Cruz, CA, USA, 23–24 February 2009.
6. Mainetti, L.; Patrono, L.; Secco, A.; Sergi, I. An IoT-aware AAL system for elderly people. In Proceedings of the 2016 International Multidisciplinary Conference on Computer and Energy Science (SpliTech), Split, Croatia, 13–15 July 2016.
7. Sun, Y.; Wang, N.; Guo, X.; Peng, Z. Understanding the acceptance of mobile health services: A comparison and integration of alternative models. *J. Electron. Commer. Res.* **2013**, *14*, 183.
8. Yan, S.; Malaney, R.; Nevat, I.; Peters, G.W. Location verification systems for VANETs in Rician fading channels. *IEEE Trans. Veh. Technol.* **2016**, *65*, 5652–5664.
9. Fraifer, M.; Fernström, M. Smart car parking system prototype utilizing CCTV nodes: A proof of concept prototype of a novel approach towards IoT-concept based smart parking. In Proceedings of the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 12–14 December 2016.
10. Agadakos, I.; Hallgren, P.; Damopoulos, D.; Sabelfeld, A.; Portokalidis, G. Location-enhanced Authentication Using the IoT: Because You Cannot Be in Two Places at Once. In Proceedings of the 32nd Annual Conference on Computer Security Applications, New York, NY, USA, 5–9 December 2016.
11. Koh, J.Y.; Nevat, I.; Leong, D.; Wong, W.-C. Geo-spatial location spoofing detection for Internet of Things. *IEEE Internet Things J.* **2016**, *3*, 971–978.
12. Khan, R.; Haque, M.; Hasan, R. A secure location proof generation scheme for supply chain integrity preservation. In Proceedings of the 2013 IEEE International Conference on Technologies for Homeland Security, HST, Waltham, MA, USA, 12–14 November 2013.

13. Muthukrishnan, K.; Lijding, M.; Havinga, P. Towards smart surroundings: Enabling techniques and technologies for localization In Proceedings of the LoCA: International Symposium on Location- and Context-Awareness, Oberpfaffenhofen, Germany, 12–13 May 2005.
14. Duckham, M.; Kulik, L. Location privacy and location-aware computing. *Dyn. Mob. GIS Investig. Chang. Space Time* **2006**, *3*, 35–51.
15. Wang, X.; Pande, A.; Zhu, J.; Mohapatra, P. STAMP: Enabling privacy-preserving location proofs for mobile users. *IEEE/ACM Trans. Netw.* **2016**, *24*, 3276–3289.
16. Zhu, Z.; Cao, G. APPLAUS: A Privacy-Preserving Location Proof Updating System for location-based services. In Proceedings of the 2011 Proceedings IEEE INFOCOM, Shanghai, China, 10–15 April 2011.
17. Lenders, V.; Koukoumidis, E.; Zhang, P.; Martonosi, M. Location-based trust for mobile user-generated content: Applications, challenges and implementations. In Proceedings of the 9th Workshop on Mobile Computing Systems and Applications, Napa Valley, CA, USA, 25–26 February 2008.
18. Khan, R.; Zawoad, S.; Haque, M.M.; Hasan, R. Who, When, and Where? Location Proof Assertion for Mobile Devices. In Proceedings of the IFIP Annual Conference on Data and Applications Security and Privacy, Vienna, Austria, 14–16 July 2014.
19. Singelee, D.; Preneel, B. Location verification using secure distance bounding protocols. In Proceedings of the IEEE International Conference on Mobile Adhoc and Sensor Systems Conference 2005, Washington, DC, USA, 7 November 2005.
20. Waters, B.; Felten, E. *Secure, Private Proofs of Location*; Technical Report; Princeton University: Princeton, NJ USA, December 2002.
21. Luo, W.; Hengartner, U. Proving Your Location Without Giving Up Your Privacy. In Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, Annapolis, MD, USA, 22–23 February 2010.
22. Hasan, R.; Khan, R.; Zawoad, S.; Haque, M.M. WORAL: A witness oriented secure location provenance framework for mobile devices. *IEEE Trans. Emerg. Top. Comput.* **2016**, *4*, 128–141.
23. Brambilla, G.; Amoretti, M.; Zanichelli, F. Using Block Chain for Peer-to-Peer Proof-of-Location. *arXiv* **2016**, arXiv:1607.00174.
24. Amoretti, M.; Brambilla, G.; Medioli, F.; Zanichelli, F. Blockchain-Based Proof of Location. In Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, 16–20 July 2018.
25. Nasrulin, B.; Muzammal, M.; Qu, Q. A Robust Spatio-Temporal Verification Protocol for Blockchain. In *International Conference on Web Information Systems Engineering*; Springer: Cham, Switzerland, 2018.
26. Neisse, R.; Steri, G.; Fovino, I.N. A Blockchain-based Approach for Data Accountability and Provenance Tracking. In Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, 29 August–1 September 2017.
27. Nosouhi, M.R.; Yu, S.; Zhou, W.; Grobler, M.; Keshtiar, H. Blockchain for secure location verification. *J. Parallel Distrib. Comput.* **2020**, *136*, 40–51.
28. Zafar, F.; Khan, A.; Suhail, S.; Ahmed, I.; Hameed, K.; Khan, H.M.; Jabeen, F.; Anjum, A. Trustworthy Data: A Survey, Taxonomy and future trends of Secure Provenance Schemes. *J. Netw. Comput. Appl.* **2017**, *94*, 50–68.
29. Zafar, F.; Khan, A.; Malik, S.U.R.; Ahmed, M.; Anjum, A.; Khan, M.I.; Javed, N.; Alam, M.; Jamil, F. A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends. *Comput. Secur.* **2017**, *65*, 29–49.
30. Camenisch, J.; Ortiz-Yepes, D.A.; Preiss, F.-S. Strengthening authentication with privacy-preserving location verification of mobile phones. In Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society, Denver, CO, USA, 12 October 2015.
31. Gabber, E.; Wool, A. How to Prove Where You Are: Tracking the Location of Customer Equipment. In Proceedings of the 5th ACM Conference on Computer and Communications Security, San Francisco, CA, USA, 3–5 November 1998.
32. Denning, D.E.; MacDoran, P.F. Location-based authentication: Grounding cyberspace for better security. *Comput. Fraud Secur.* **1996**, *1996*, 12–16.
33. Capkun, S.; Hubaux, J.P. Secure positioning of wireless devices with application to sensor networks. In Proceedings of the IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies, Miami, FL, USA, 13–17 March 2005.

34. Zugenmaier, A.; Kreutzer, M.; Kabatnik, M. Enhancing applications with approved location stamps. In Proceedings of the IEEE Intelligent Network 2001 Workshop. IN 2001 Conference Record (Cat. No.01TH8566), Boston, MA, USA, 6–9 May 2001.
35. Gruteser, M.; Grunwald, D. Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking. In Proceedings of the 1st International Conference on Mobile Systems, Applications and Services, San Francisco, CA, USA, 5–8 May 2003.
36. Bauer, K.; McCoy, D.; Anderson, E.; Breitenbach, M.; Grudic, G.; Grunwald, D.; Sicker, D. The Directional Attack on Wireless Localization. In Proceedings of the GLOBECOM 2009–2009 IEEE Global Telecommunications Conference, Honolulu, HI, USA, 30 November–4 December 2009.
37. Brassil, J.; Netravali, R.; Haber, S.; Manadhata, P.; Rao, P. Authenticating a mobile device's location using voice signatures. In Proceedings of the 2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, Spain, 8–10 October 2012.
38. Saroiu, S.; Wolman, A. I Am a Sensor, and I Approve This Message. In Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, Annapolis, MD, USA, 22–23 February 2010.
39. Gilbert, P.; Cox, L.P.; Jung, J.; Wetherall, D. Toward Trustworthy Mobile Sensing. In Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, Annapolis, MD, USA, 22–23 February 2010.
40. Luo, W.; Hengartner, U. Veriplace: A privacy-aware location proof architecture. In Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems, San Jose, CA, USA, 3–5 November 2010.
41. Hasan, R.; Burns, R. Where have you been? Secure location provenance for mobile devices. *arXiv* **2011**, arXiv:1107.1821.
42. Davis, B.; Chen, H.; Franklin, M. Privacy-preserving Alibi Systems. In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, Seoul, Korea, 2–4 May 2012.
43. Ananthanarayanan, G.; Haridasan, M.; Mohomed, I.; Terry, D.; Thekkath, C.A. StarTrack: A Framework. for Enabling Track-based Applications. In Proceedings of the 7th International Conference on Mobile Systems, Applications, and Services, Kraków, Poland, 22–25 June 2009.
44. González-Tablas, A.I.; Ramos, B.; Ribagorda, A. Path-Stamps: A Proposal for Enhancing Security of Location Tracking Applications. In Proceedings of the CAiSE Workshops, Klagenfurt/Velden, Austria, 16–20 June 2003.
45. Khan, R.; Zawoad, S.; Haque, M.M.; Hasan, R. OTIT: Towards Secure Provenance Modeling for Location Proofs. In Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security, Kyoto, Japan, 3–6 June 2014.
46. Bucher, D.; Rudi, D.; Buffat, R. Captcha Your Location Proof—A Novel Method for Passive Location Proofs in Adversarial Environments. In Proceedings of the LBS 2018: 14th International Conference on Location Based Services, Zurich, Switzerland, 15–17 January 2018.
47. Talasila, M.; Curtmola, R.; Borcea, C. Link: Location verification through immediate neighbors knowledge. In Proceedings of the International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services, Sydeny, Australia, 6–9 December 2010.
48. Stojkoska, B.R.; Kosovic, I.N.; Jagust, T. A Survey of Indoor Localization Techniques for Smartphones. In Proceedings of the 8th International Conference ICT Innovations 2016, Ohrid, Macedonia, 5–7 September 2016.
49. Yu, D.-Y.; Ranganathan, A.; Masti, R.J.; Soriente, C.; Capkun, S. W-SPS: Designing a Wide-Area Secure Positioning System. *IACR Cryptol. Eprint Arch.* **2015**, *2015*, 230.
50. Miettinen, M.; Asokan, N.; Koushanfar, F.; Nguyen, T.D.; Rios, J.; Sadeghi, A.-R.; Sobhani, M.; Yellapantula, S. I Know Where You Are: Proofs of Presence Resilient to Malicious Provers. In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, Singapore, 14–17April 2015.
51. Javali, C.; Revadigar, G.; Rasmussen, K.B.; Hu, W.; Jha, S. I Am Alice, I Was in Wonderland: Secure Location Proof Generation and Verification Protocol. In Proceedings of the 2016 IEEE 41st Conference on Local Computer Networks (LCN), Dubai, UAE, 7–10 November 2016.
52. Deak, G.; Curran, K.; Condell, J. A survey of active and passive indoor localisation systems. *Comput. Commun.* **2012**, *35*, 1939–1954.
53. Wang, W.; Chen, Y.; Zhang, Q. Privacy-Preserving Location Authentication in Wi-Fi Networks Using Fine-Grained Physical Layer Signatures. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 1218–1225.

54. Pham, A.; Huguenin, K.; Bilogrevic, I.; Hubaux, J.-P. Secure and Private Proofs for Location-based Activity Summaries in Urban Areas. In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Seattle, WA, USA, 13–17 September 2014.
55. Mengjun, L.; Shubo, L.; Rui, Z.; Yongkai, L.; Jun, W.; Hui, C. Privacy-preserving distributed location proof generating system. *China Commun.* **2016**, *13*, 203–218.
56. Dupin, A.; Robert, J.-M.; Bidan, C. Location-proof system based on secure multi-party computations. In Proceedings of the 12th International Conference, ProvSec 2018, Jeju, Korea, 25–28 October 2018.
57. Brassil, J.; Manadhata, P.K. Proving the location of a mobile device user. In Proceedings of the 4th International Conference, MobiSec 2012, Frankfurt am Main, Germany, 25–26 June 2012.
58. Subhashri, C.; Vijayalakshmi, P. Enabling collusion resistant location proof and secure location sharing for mobile users. *Adv. Nat. Appl. Sci.* **2017**, *11*, 62–72.
59. Hu, H.; Chen, Q.; Xu, J.; Choi, B. Assuring Spatio-Temporal Integrity on Mobile Devices with Minimum Location Disclosure. *IEEE Trans. Mobile Comput.* **2017**, *16*, 3000–3013.
60. Ni, X.; Luo, J.; Zhang, B.; Teng, J.; Bai, X.; Liu, B.; Xuan, D. A mobile phone-based physical-social location proof system for mobile social network service. *Secur. Commun. Netw.* **2016**, *9*, 1890–1904.