IoT

MDPI

Article

Secure Path: Block-Chaining IoT Information for Continuous Authentication in Smart Spaces

Lorenzo Bracciale [1,†], Pierpaolo Loreti [1,*,†], Claudio Pisa [1] and Alex Shahidi [2]

[1] Department of Electrical Engineering, University of Rome "Tor Vergata", 00133 Rome, Italy; lorenzo.bracciale@uniroma2.it (L.B.); claudio.pisa@uniroma2.it (C.P.)
[2] EntirID LLC, Silicon Valley Cybersecurity StartUp, Cupertino, CA 95014, USA; alex@entirid.com
* Correspondence: pierpaolo.loreti@uniroma2.it
† These authors contributed equally to this work.

Abstract: The Internet of Things offers a wide range of possibilities that can be exploited more or less explicitly for user authentication, ranging from specifically designed systems including biometric devices to environmental sensors that can be opportunistically used to feed behavioural authentication systems. How to integrate all this information in a reliable way to get a continuous authentication service presents several open challenges. Among these: how to combine semi-trusted information coming from non-tamper-proof sensors, where to store such data avoiding a single point of failure, how to analyse data in a distributed way, which interface to use to provide an authentication service to a multitude of different services and applications. In this paper, we present a Blockchain-based architectural solution of a distributed system able to transform IoT interactions into useful data for an authentication system. The design includes: (i) a security procedure to certify users' positions and identities, (ii) a secure storage to hold this information, and (iii) a service to dynamically assign a trust level to a user's position. We call this system "Secure Path".

Keywords: continuous authentication; IoT authentication; smart space; security; Blockchain

check for updates

Citation: Bracciale, L.; Loreti, P.; Pisa, C.; Shahidi, A. Secure Path: Block-Chaining IoT Information for Continuous Authentication in Smart Spaces. *IoT* **2021**, *2*, 326–340. https://doi.org/10.3390/iot2020017

Academic Editors: Paul Vickers and James Nicholson

Received: 31 March 2021
Accepted: 29 April 2021
Published: 18 May 2021

1. Introduction

The technological and economic boost of the IoT world is pushing a rapid transformation of the environments around us into connected, intelligent smart spaces. Houses, vehicles, hospitals, and cities are becoming more comfortable, energy-efficient, and secure thanks to IoT solutions. With the term "smart spaces", we refer to physical environments where humans and technology can interact with each other enabling an immersive experience for the user. In such environments, there is a continuous interaction between the user and the environment and a continuous exchange of data. Clearly, all this information can also be used for authenticating users to different systems, but, as a matter of fact, this rarely happens today due to the big (open) issue of interoperability among different IoT devices and systems. Consider, for example, a smart office where employees must pass their security badges to access the facility, use their smart keys to open their room, and then log in to their PC with their credentials. Even though these systems are usually connected to the Internet, information is not shared; for instance, the login method on the PCs remains the same also in the suspicious case when nobody ever entered the room. In this work, we want to present an authentication framework for users of smart spaces. If combined with indoor/outdoor localisation, this system aims to minimise the number of authentication requests and keep a persistent authentication status related to the user and its current position.

Indeed, if we are confident enough that a given user is in a given location, we can then completely rethink the way users interact with the environment, introducing seamless service access and context-aware computing [1], raising productivity, usability, and comfort. For example, automatically unlock doors, automatically log in when the user sits in front of a laptop, automatically redirect video, phone calls and multimedia to the screen nearest to the user's current position, and automatically regulate the smart space to be more comfortable for the user by acting on temperature and lighting preferences.

1.1. Persistent Location-Based Authentication: Are We There Yet?

Technological advances in indoor navigation systems allow fine-grain localisation (up to 12 cm with the current ultra-wide band (UWB) technology [2], with 5G networks [3]) using small-form-factor chips and relatively cheap infrastructure. This makes the integration feasible in mobile phones or smart badges. At the same time, users can be continuously associated with their devices through advanced biometric systems, with sophisticated authentication techniques, such as face recognition, fingerprint, and vein fingerprinting [4].

Therefore, how far are we from a fully-fledged authenticated position system? From our perspective, the true problem is in the "level" of trust required of the identity (e.g., biometric spoofing), of the position (e.g., wormhole attacks), and of their association (e.g., impersonation attack), given that almost any system can be hacked. However, in smart spaces, the effectiveness of many attacks can be greatly mitigated thanks to the numerous IoT interactions that can be *chained* together to achieve a higher level of trust, just like multi-factor authentication (MFA) combines different pieces of evidence. We built our solution on this basis coupled with the possibility of creating "on demand" challenges.

1.2. IoT Interoperable Authentication

Different systems require different levels of security. Accessing a PC is different from buying a coffee at the vending machine, although both of them require the user to authenticate themself (e.g., inserting her credentials on PC or using her NFC card for the vending machine). For this reason, we propose to decouple these two aspects: we have an authentication information base (AIB), which collects all the interactions of the user with the smart environment, and an authentication algorithm, which runs on top of such information, to determine the level of trust we assign about the pair user identity/user position. Applications can simply look at the output of the algorithm and, if the level of trust is suitable for that specific service, authenticate the user. Otherwise, users may be asked for further proof (we call them on-demand authentication challenges), for instance, to log in with username–password. Users' answers to such challenges will be logged as well in the AIB and raise (or decrease) the trust level associated with the user.

Although the problem of continuous authentication and location-based authentication has been tackled in the literature for a long time, we approach the problem under a different perspective. We do not provide any specific algorithm for using IoT data to authenticate users through their pattern (e.g., [5]), nor do we rely on trusted architectural elements to determine the current user position [6].

Conversely, we fully embrace the trust uncertainty and just pile up untrusted environment IoT data but in an accountable manner (we are using device signature, multi-signature, and Blockchain for that, as explained later on), considering that a pervasive multi-vendor and heterogeneous IoT deployment offers a natural protection against attacks that can hardly take control of all the different subsystems.

Our key questions are thus: to what extent can we "certify" that a given user is in a given position at a given time? How to implement a variable user authentication level that changes over the time? How to use the authentication information in practical applications? And, finally, is it possible to provide all of this without any trusted third parties?

1.3. Our Contribution: Secure Path

In this work, we present a solution to exploit the cyber-physical interactions of the IoT with the ultimate goal of presenting a new use case of delivering persistent location-based authentication in smart spaces.

Our research questions are: (i) how to combine semi-trusted information coming from non-tamper-proof sensors; (ii) where to store such data avoiding a single point of failure;

(iii) how to analyse data in a distributed way; and (iv) which interface to use to provide an authentication service to a multitude of services and applications.

To answer these questions, we propose a solution called "Secure Path", which provides answers to such questions using the following elements:

- *A security procedure designed* to co-certify users' positions and identities by means of cyber-physical interactions: The certification/co-certification of sensed data allows to introduce a first level of trust (non-repudiation), i.e., be sure that data are coming from a given source. However, we still have uncertainty if the sensing device or the data on the receiving server has been tampered with. This point is addressed in the next elements.
- *A secure storage to hold information, called authentication information base (AIB)*: Relying on Blockchain (and in particular on data streams), we guarantee immutability of the data and prevent attacks on the server, avoiding a single point of failure.
- *A service to dynamically evaluate the trust level of a user's position*: We implemented a distributed service called trust committee to evaluate information inside the AIB and periodically estimate the level of trust about user identity and position. This trust level changes over time, according to the interactions that users perform with the environment (e.g., open a door with a smart card, or pass nearby the security guard). The committee is built on top of the Blockchain, using consensus to prevent software modifications. The evaluation of the trust committee is written in the Blockchain and can be used by applications and services for authentication purposes.

These elements are used to devise a distributed architecture aimed at reaching the ultimate goal: knowing who is where, at any time, with a given degree of trust. This results in obtaining the tuple: who, where, when, how sure we are. Our "Secure Path" solution assigns a certain level of trust to the position inside a smart space depending on a user's history.

The rest of this work is structured as follows. Section 3 explains the basic elements of the design, Section 4 lists the different operations all entities described in the architecture need to perform, and Section 5 contains a proof-of-concept of the proposed system. Finally, conclusions are drawn.

2. Related Work

2.1. Identity-Management Systems

Identity management, in the context of continuous and pervasive authentication, has received paramount attention from many security researchers, who tackle the problem under several and different perspectives. The problem is indeed a complex mix of security, deployability/industrialisation, and usability aspects, intertwined together in domain specific contexts.

Solutions based on dedicated hardware try to provide continuous authentication and aggregate the current need of having a large number of credentials. For instance, Pico [7] proposes a personal device connected to a set of personal/wearable sensors (glasses, belt, etc.) in which a master key distributed on these items with secret sharing offers protection against thief/loss of the personal device. Solutions based on software try to minimize the number of credentials asked of users and to understand when it is possible to operate with implicit authentication. This concept has been carried out by progressive authentication initially proposed by [8].

Other solutions use the additional position factor of authentication in scenarios where physical presence is required, by estimating the likelihood a user is in a given place "because you cannot be in two places at once" [9], also making use of the pervasive IoT environment [10].

In this work, we combine parts of these approaches in a framework characterised by a strong decoupling of the collection of data and the processing of such data. The ability of accessing the outcome of such processing by different applications enables implicit authentication. Likewise, in the proposed framework, if the level of trust is not suitable with the specific service or application needs, they can ask users for further challenges to raise the trust the system has about their identity or position.

An approach similar to this one is presented in [11], which explores an architecture for providing multi-factor authentication as a service by introducing a loose coupling and separation of duties between network entities and end user devices.

2.2. Industrial Solutions

Gemalto SafeNet Authentication service offers the authentication as a service (AaaS) solution to organisations, providing easy-to-apply multi-factor authentication for securing access to any application, from any device, anywhere. The system relies on a massive series of integrations (currently more than 150), with a broad choice of 2FA methods and tokens, management systems, and services.

UniquID (https://uniquid.com/, accessed on 17 May 2021) is a startup that uses Blockchain and smart contracts for building a peer-to-peer trust model for IoT to overcome the limitation of centralised authentication and thus the possibility that the centralised system can be compromised. It uses PGP and web-of-trust for (self) key generation and regulates the interactions among machines through smart contracts. A public key of the administrator grants him the remote control of the device.

2.3. Multi-Factor Protocols

Human interaction with IoT devices demands authentication procedures that need to be seamless and user-friendly but at the same time highly secure. Thus several MFA schemes have been designed to find a trade-off between security and usability. However, designing a secure MFA scheme for IoT environments is a hard challenge, and several schemes present serious security flaws [12]. Indeed, the integration of mobile terminals into the IoT system, on the one hand, simplifies some authentication procedures but, on the other hand, poses additional issues for the security of the system. In many cases, it is necessary to increase the number and type of factors required for authentication, as proposed in [13]. Strong authentication protocols have to be used for healthcare applications based on IoT devices since highly sensitive data can be exposed to attacks. Thus, in [14], a three-factor authentication protocol, including a password, biometrics, and a smartcard, is proposed to authenticate the medical professional protecting the patient's medical data. In this case, the access control and the data sharing is demanded by a cloud service that needs to be trusted.

2.4. Blockchain-Based Solutions

Blockchain is a decentralised database allowing "parties who don't fully trust each other to form and maintain consensus about the existence, status and evolution of a set of shared facts". It has been recently used by several companies for different purposes. For what concerns trust and identity access management (IAM), in many cases, it has been used for the so-called "self-sovereign identity networks". The concept referred to as self-sovereign identity consists of storing identities that could potentially be used across different services but also leave a person the control of their information [15].

Several solutions have been proposed for self-sovereign identity networks, such as:

- Sovrin, proposed by a non-profit foundation, is a system based on a permissioned Blockchain where only trusted entities are allowed to write to the ledger.
- uPort offers a solution for the same problem but relies on a smartphone app that embodies the principles of self-sovereign identity.
- Alastria is a "national Blockchain ecosystem" used by Spain and based on a semi-public permissioned Ethereum-based Blockchain to support services with legal effectiveness.
- Hyperledger's Indy project covers decentralised identity providing tools, libraries, and reusable components for creating and using independent digital identities rooted on Blockchains.

For what concerns IoT, Blockchain technologies can provide interoperability across heterogeneous devices, covering and complementing IoT systems on different aspects from security [16] to authentication of devices [17] to providing secure data storage and recovery ability in an industrial context [18]. Dedicated systems for the Internet of Everything, such as IOTA, have been recently proposed, and researchers demonstrate the feasibility of implementation of "light nodes" [19], compatible with the energy and computation requirements of Industrial IoT.

Finally, it is also worth mentioning the recent effort of the World Wide Web Consortium (W3C) Verifiable Claims Working Group, whose goal is to enable external verification of claims, regardless of where they are stored, which is in the same direction as this work.

3. Concept and Design

We define "Secure Path" as a certified and immutable track of a person inside a controlled premise. It includes a time series of spatial positions, successful and unsuccessful authentications, specific actions, and relevant contextual information acquired through IoT. This represents an information base that can be used by algorithms for authentication and/or seamless user authorisation.

3.1. Security Challenges in a Smart Environment

The interactions of people immersed in a smart environment are numerous and continuous. The majority, though, do not represent a good system to authenticate a user because they were not specifically designed for that aim (e.g., switch on the light, adjust room temperature). Usually, behavioural analysis is used to support rather than substitute a proper authentication technology [20]. Even security-designed interactions (that we broadly refer to as "challenges"), such as face recognition and access badge scanning, do not usually offer a service that can provide authorisation towards other services/systems. Neither do they have native chaining mechanisms for other challenges. As an example, consider a user entering inside their office, opening the door with a smart key, and then logging on to their laptop. These two challenges (proof of possession of the smart key and proof of knowledge of login/password to access to the laptop) are usually independent and confined to one specific application or service (open the door, accessing to the laptop). Conversely, they can be linked together to provide a greater level of security according to the same principle that is the base of the multi-factor authentication (MFA). As a matter of fact, even integrated IoT services sometimes lack specific integration for security, authorisation, and authentication tasks. This is particularly clear in the global real-world multi-vendor smart space scenario where mutual information exchange is more challenging.

To overcome this hurdle, the "Secure Path" solution envisions a smart space in which IoT devices act as independent and autonomous certification authorities able to confirm user identity and position. This is possible, for example, by binding each IoT device with a different cryptography key and using the keys to sign the interactions of the devices with a user. This data comprises the type of IoT device (e.g., camera), the challenge the user passed (e.g., face recognition), and the information on time, user, and location. All of this information is collected in an information base described in the next subsection to allow "challenge" chaining. As a result, an attacker must tamper with all IoT devices/systems in order to fool the "Secure Path" since there is no central authority.

By exploiting the challenge mechanism, "Secure Path" aims to bind the IoT information together, bringing continuity and persistence, so as to make it more difficult to perform an identity theft in-between. At the same time, the union of multiple authentication techniques and systems reinforces the strength of each technique. Indeed, as in the case of MFA, the combination of multiple techniques performs better than the sum of the parts as the spoofing/theft of any factor does not compromise the whole system's validity. The usage of spatial and temporal information about the user prevents session hijacking. As a matter of fact, while conventional authentication mechanisms such as Single sign-on (SSO) assume that the legitimate user is the one who accesses the service throughout the entire access session [21], for IoT devices the concept of a valid authentication time period needs more attention since it affects the robustness and the technical feasibility of authentication [22].

With specifically designed physical layer challenges (for instance, based on Shannon's information-theoretic security [23]), location-based attacks like location spoofing or wormhole attacks can be prevented (or made more difficult to perform).

3.2. Environmental Interactions with Blockchain

A Blockchain is a growing list of records called blocks. Each block contains the hash of the previous block and contains transaction data to perform an asset exchange between two or more parties identified by their addresses. By design, a Blockchain is resistant to modification of its data because once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks. A Blockchain can be seen as an ordered list of items digitally signed by one or more publishers and can be used as a general purpose append-only database, providing timestamping, notarisation and immutability. Moreover, some data can be directly added in the block, i.e., embedded in the transaction, or can be referenced by the transaction (represented, for example, by the data hash).

The "Secure Path" makes use of the Blockchain to collect interactions among users and the device in the environment as signed transactions, as shown in Figure 1. Each device has a unique address and, by using its key, is able to digitally sign the information that is published in the blocks. For example, the user can publish their GPS position or information on the wireless networks that they detect. The devices and the systems in the environment can publish their interactions with the user. For instance, if the user is recognised by a biometric system or controls a smart appliance, these interactions can be published either by the user or by the IoT devices and made available to other systems.

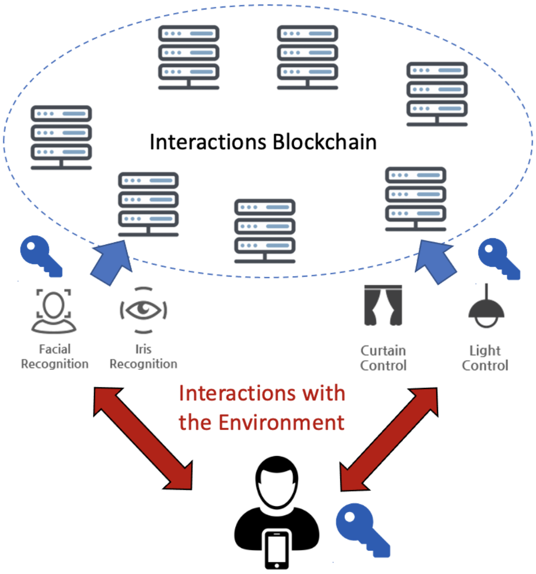


Figure 1. Secure Path: interactions among users and IoT devices are signed and stored in the Blockchain.

Note that some kinds of transactions may need the approval of two or more actors, e.g., the user and the device. To cope with this requirement, it is particularly convenient to use multisignature addresses (multisig) in the Blockchain, which are identities collectively managed by multiple parties. For instance, Bitcoin defines "m-of-n" multisignatures when it requires that at least m private keys must sign a transaction of the n addresses in the multi-address. In the "Secure Path", we used 2-of-2 multisig, where each of the two separate parties must approve the transaction.

3.3. Authentication Information Base

In our design, we chose to decouple authentication evaluation from information collection by introducing an authentication information base (AIB). This is a trusted storage whose role is to hold information needed to evaluate authentication. This information base is mission critical since it must collect heterogeneous information from different (non-tamper-proof) IoT devices and systems and, at the same time, offer resiliency against attacks (on the information base or to the authenticator method), which could invalidate the whole process.

For this reason, we chose to implement AIB using a permissioned Blockchain. Indeed, a Blockchain allows "parties who don't fully trust each other to form and maintain consensus about the existence, status and evolution of a set of shared facts", in our case, the outcome of the IoT interactions and the security challenges.

Even though the information committed can come from untrusted sources, the information base cannot be manipulated, and given that the information is digitally signed with cryptographic signatures, it cannot be repudiated. Indeed, the system can resist attacks that can compromise even $N/2 - 1$ of the servers and can detect attacks provided that at least one server is not involved in the attack. This offers extra protection against internal cyber-security threats aimed at compromising the information base rather than at the single authentication procedure. As a matter of fact, more than 50% of attacks are carried out by insiders (According to IBM 2016 Cyber Security Intelligence Index, 60% of attacks started with insiders). Blockchain validation prevents devices committing unauthorised transactions according to the rules defined by the chain and prevents attackers covering their tracks through its append-only structure and distributed nature.

Blockchain logs the "Secure Path" information so the system leverages the integrity of the information and the resiliency of the system to attacks, thanks to its ability to archive data in a non-modifiable and non-erasable manner.

In the Blockchain, IoT devices and systems publish the following information:

1. User positions: user devices periodically publish self-signed locations.
2. Outcomes of the challenges: interactions with the IoT world are committed to the Blockchain. Data can be certified only by the environment (e.g., a camera that recognises a face) or can be co-certified by the user's device using multi-signature (e.g., users scanning their access badges).
3. Evaluation of the user trust level (detailed in the next section).

3.4. User Trust Level and Trust Committee

In the "Secure Path" solution, the authentication information base can be used to numerically evaluate the level of trust to assign to a user's assertions: they are who they claim to be, at the position they claim to be, and at the time they declare. We call this number the trust level. The algorithm that evaluates the trust level uses certified data published in the Blockchain with insights about the user's claimed position/identity according to the type of interaction (security/non-security), the type of signature (self-certified or co-certified), and the specific history of interactions. In general, this algorithm can be arbitrarily complex and might be domain/environment specific, as also pointed out by [24]. For instance, a user's trust level may increase if they have many co-certified interactions and may decrease as time passes or when they move away from their usual path.

The trust level evaluation algorithm is executed by an authenticator system that provides an authentication service running periodically and on demand. The algorithm's numerical output is written to the AIB. IoT applications can read these values and decide on seamless authorisations according to their internal policy (e.g., if the trust level is greater than five, open the door when a given user is approaching).

To prevent attacks to the authenticator and to offer a higher level of resiliency, we propose that the identity verification/estimation be carried out by a trust committee. This is a set of N agents, sharing the same logic, deployed in different companies, that write to the Blockchain (Figure 2). The goal of each member is to provide a value that numerically describes the estimation of trust associated with a user in the range 0–10. An N/M logic, i.e., it suffices that N members over the total M decide for a given trust level to commit it to the chain, offers protection against attacks to single members of the committee. In this framework, the trust committee service can be built using conventional multi-signature techniques available in the Blockchain.

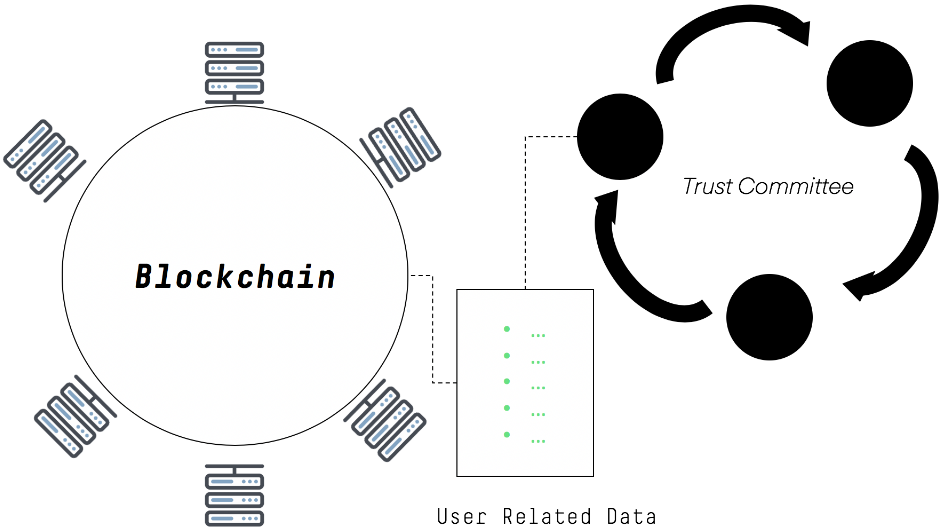


Figure 2. The trust committee takes user-related data from the Blockchain and commits an estimation of the user's trust value.

3.5. Design Summary

In brief, the "Secure Path" solution works as follows:

- Users are equipped with smart-badges that periodically communicate the identity and position of the user holding the device.
- IoT devices can co-certify information about a user's claimed position, time, and identity when the user interacts with them.
- Information is stored in the AIB implemented with Blockchain technology.
- A distributed service, called the trust committee, processes the AIB to evaluate the possibility of that specific user being in that specific place at that moment and publishes a trust level. The trust level basically increases with the number of challenges overcome (i.e., authentication procedures/interactions) and decreases in time and space. This is dynamically regulated by the trust committee algorithm, which is domain specific.
- An application or service may implicitly authenticate a user by retrieving the current trust level from the Blockchain. If the current trust level is enough for that service, users can be implicitly authenticated. Otherwise, they can be demanded to raise their trust level by presenting some more pieces of evidence (factors), e.g., asked for a user password.

4. Use Case

Let us describe the operations in the "Secure Path" using as an example the facility and the path illustrated in Figure 3. We assume that a user that enters the smart space is equipped with a user device (UD). A UD can be a smart-badge or a wearable device, such as a wristband with indoor localisation technology (e.g., Decawaves DW1000 UWB module), RF communication (e.g., Bluetooth, 5G) and, optionally, bio-metric authentication (e.g., vein scanner) for scenarios demanding an extremely high level of security.

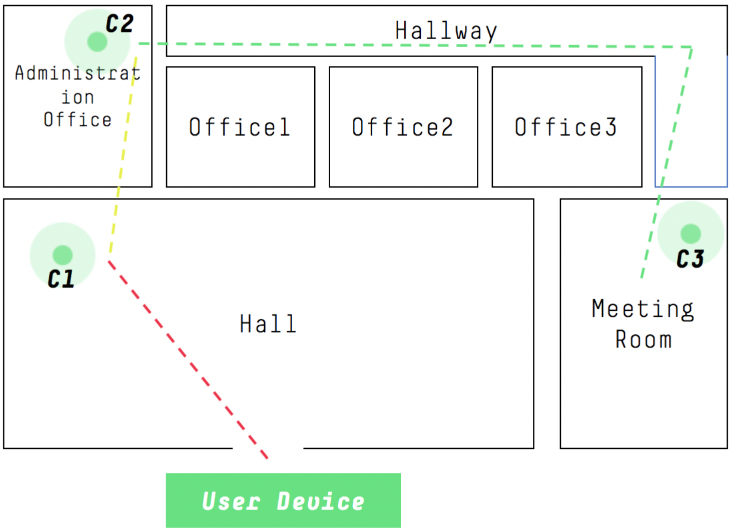


Figure 3. Example of a "Secure Path": user passes through checkpoints C1, C2, and C3.

The UD periodically commits its position to the Blockchain. We call this message self position information (SPI). It contains the self-declared position signed with the user's (bio-metric) key. Then let us suppose the user passes near a guard post (checkpoint C1) controlled by a "guard" that can either be automated or be a person. The guard physically checks the person's credentials (e.g., ID card). If the check passes, the checkpoint operator co-signs, using a multi-signature, the UD's position. The Blockchain registers this message together with the type of check performed (e.g., "check-type: CHECK-ID-CARD"). Time and position are both declared. This information is written in the user's "Secure Path" in the form of a certified position information (CPI) message.

Then the user is allowed to enter the administration office where the access badge will be verified at checkpoint C2. Once passed this check, C2 operator may verify if the user passed C1 less than 15 min ago and may refuse to co-sign the data if this verification fails. In this case, C2 commits the reason of its choice to the Blockchain. Suppose the user also passes C2 and then goes down the hallway and reaches the meeting room. Here, the user's face is captured by the security camera and will be recognised by a face detection algorithm. Accordingly, C3 decides to sign another CPI.

In the meeting room, the user wants to use a desktop computer. The software on that computer contacts the TCS that returns 8.5 as the current trust value assigned to the UD. Therefore, the operating system decides not to ask for the password and permits an automatic log in. Alternatively, the computer may ask the user for a password and eventually log the result of the challenge to the Blockchain, becoming checkpoint C4.

Certified Positions with Checkpoint Multi-Signature Verification

Once the UD is challenged by a checkpoint, a multi-signature transaction flow begins, as described in the flow diagram represented in Figure 4. In particular, the user and the checkpoint need to know their mutual address (hash of their public keys). Then, the user can create a multi-signature address on-demand, involving both identities. After that, the user emits a signature request for the checkpoint (Sign 1/2). According to its internal logic, the checkpoint may agree to fulfil the request, co-sign the transaction, and send the signed message back to the user. Finally, the user completes the transaction with his signature (Sign 2/2). At this point, the user can transmit the transaction to be appended to the Blockchain.

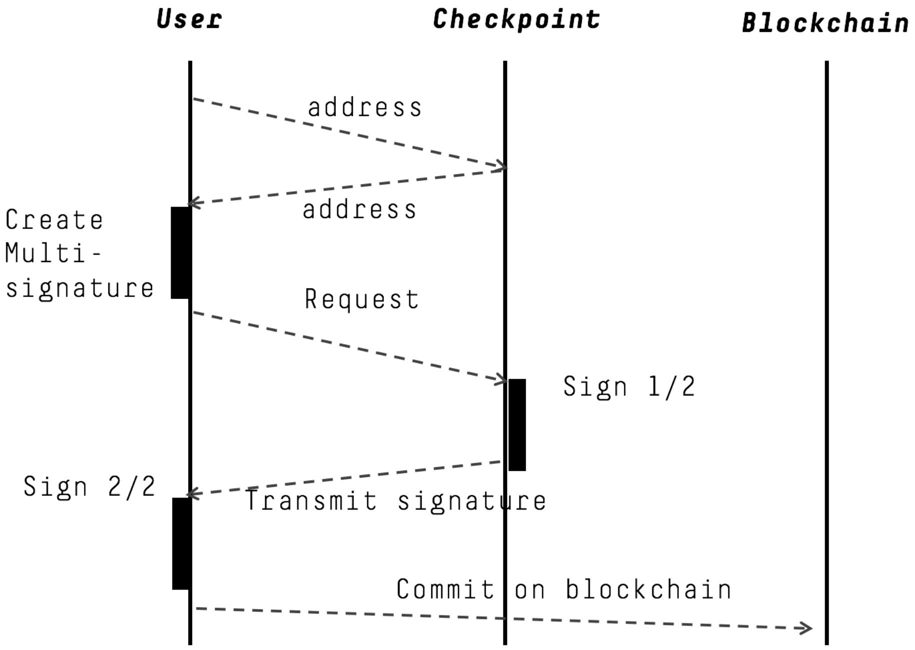


Figure 4. Multi-signature flow diagram.

5. Proof of Concept

We developed a proof-of-concept of the proposed system using a smartphone and substituting, for implementation convenience, the indoor positioning system with the outdoor positioning system given by the smartphone's GPS.

The proof of concept (PoC) is composed of the following entities:

- **Authentication information base**: We set up a Blockchain composed of two nodes, built on top of Multichain (https://www.multichain.com/, accessed on 17 May 2021).
- **Mobile application**: This emulates the User Device, using GPS as a position source and committing SPI and CPI to the chain through the mobile network.
- **Web application server**: We built an application server that allows the creation/ monitoring of the checkpoint status and exposes a set of APIs needed by the mobile application to interact with the infrastructure.
- **Trust Committee**: A replicated algorithm that periodically writes to the chain a trust value based on the history of the user device's interactions.

5.1. Blockchain Organisation

We exploited Multichain data streams to create one stream for each user. Then, we granted read/write access rights to users only for their own streams. A data stream is composed of items where each is represented by a Blockchain transaction. Stream items have a timestamp (taken from the header of the block in which the item is confirmed), payload data, one or more publishers who have digitally signed the item, and an optional key to ease retrieval, which we set as the user ID. An example of a stream item associated with "user1" is reported in Figure 5.

To the same stream, checkpoints can commit multi-signed transactions involving both user and checkpoint keys. These transactions are also identified by the "checkpoint's" key.

We created an extra stream for the trust committee (TC) named "tcs", where we give the TC implementation read/write access rights. The TC periodically publishes its trust evaluation of a user to this stream according to a simple algorithm. We implemented a simple time decay trust evaluation model where we linearly decrease a user's trust as time passes from the most recent CPI received. Far more advanced algorithms can be engineered on the available data, but their design is beyond the scope of this work.

```
"publishers" : [
"1W9AwFKE34wLJJaxCRLQf9RRh..."
],
"keys" : [
"user1"
],
"data" : "12121212121289898989",
"confirmations" : 15,
"blocktime" : 1529506659,
"txid" : "24e5e7292851cc00e..."
```

Figure 5. Example of a stream item associated with "user1".

5.2. Mobile Application

The mobile application was built to emulate the user device. The application was implemented through an Android App, using the GPS as a location source for (outdoor) position information. The application shows user information on a map, takes care of committing the transactions using the web application server, allows interaction with checkpoints to increase the trust level, and shows the user information committed to the Blockchain. Some screens of the application are reported in Figure 6.

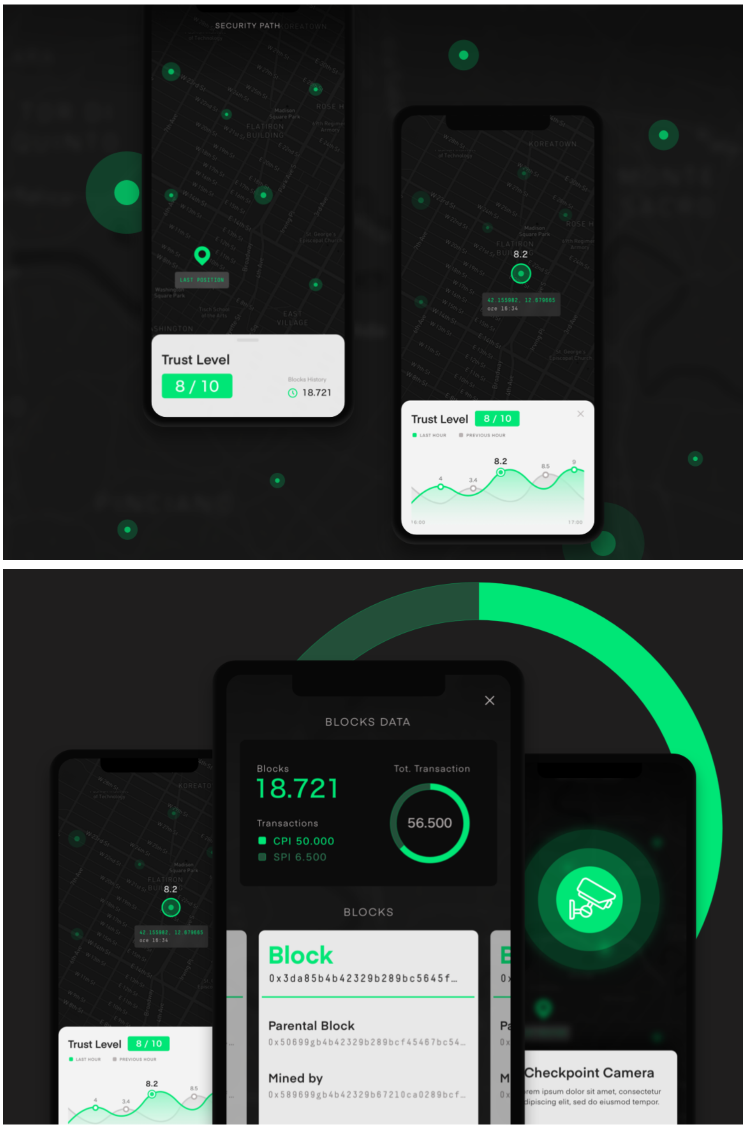


Figure 6. Mobile application built as a proof of concept.

5.3. Web Application Server

The web application server exposes a set of APIs to the mobile application and offers an interactive web page to manage checkpoint positions.

The application was built using the Flask python microframework (http://flask.pocoo.org/, accessed on 17 May 2021).

6. Evaluation and Discussion

Two natural questions that may arise about the proposed solution are: (i) is it feasible, and (ii) how is this solution better/different with respect to the state-of-the-art? In this section, we provide an analysis of these two fundamental points. Specifically, in Section 6.1, we evaluate the feasibility of constructing a "Secure Path" inside a smart office, starting from the current available technology of smart badges. Then, we asked whether the energy capacity of a smart badge is compatible to accommodate indoor/outdoor localisation service to support users during business hours and the necessary networking/processing activities. Section 6.2 is devoted to a discussion of the level of security introduced by the proposed approach and to benchmark the characteristics of the "Secure Path" with respect to the state-of-the-art.

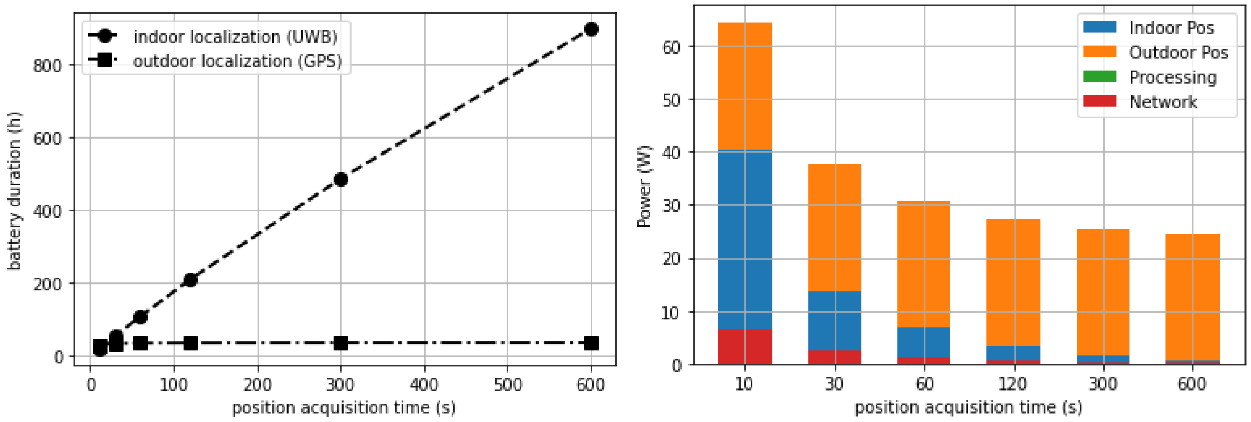
6.1. Energy Evaluation

We evaluated the energy consumption of a possible implementation of the smart badge as a standalone device. To this aim, we considered the most important hardware components that characterise the device, which are:

- **Indoor localisation**: We considered a Decawave DWM1001 Tag operating within the infrastructure range with 500 µs as response time. To derive the average energy consumption (which depends on the time between ranges), we considered a typical state machine cycle as reported in the datasheet Startup, Tx Poll Preamble, Tx Poll Data, Tag idles before turning on Rx, Rx Preamble hunt, Rx Response Preamble, Rx Response data, Tag idles and before turning on Tx, Tx Final Preamble, Tx Final Data, Return to Deep Sleep.
- **Outdoor localisation**: We considered an energy-efficient GPS implementation (Gms-u1LP) that operates in tracking mode all of the time to avoid energy and time expensive position acquisitions (35 s cold start vs. 1 s for hot start).
- **Processing**: We considered an ultra low power SoC, Texas Instrument CC430, and assume a relatively high duty cycle of 0.1 to take into account the cryptographic operations workload.
- **Networking**: We considered the Narrowband IoT (nb-IoT) technology, whose energy consumption has been evaluated in the field in [25]. We used the energy model proposed by [25], assuming a packet size of 800 bytes. We considered nb-IoT instead of the wireless data communication provided by the DWM1001 as exhibiting a better trade-off among power consumption and an achievable data rate. Moreover, it allows data communication also beyond the coverage range of the UWB indoor localisation infrastructure.
- **Battery capacity**: We considered a battery capacity of 850 mAh, which is reasonable for a smart badge application, as already applied in commercial products (e.g., Abeeway Smart Badge).

In the analysis, we varied the position acquisition time, i.e., the time among two successful and subsequent position acquisitions (either in an outdoor or indoor scenario).

Figure 7a shows the duration of the battery (in hours) when all the previously described hardware is powered by the 850 mAh battery. Clearly, more energy will be required to power all the required circuitry that depends on the specific hardware design (e.g., DCDC converter). However, as we can see from the figure, the energy consumption of the major components is more than enough to allow one charge per week if the position acquisition interval chosen is bigger than 30 s. Figure 7b shows the energy budget breakdown of all the components, varying the position acquisition time. As we can see, the UWB positioning concurs for the greatest part in the energy consumption when frequent indoor location is performed, but its impact can be radically reduced by adopting less frequent position updating, such as one per minute.



(**a**) (**b**)

Figure 7. Energy consumption of the main electronic component of the smart badge. (**a**) Battery duration with indoor and outdoor localisation. (**b**) Energy budget breakdown.

6.2. Comparison

The proposed architecture “chains” different and existing authentication systems (e.g., login/password, biometric systems, AI face recognition, and behaviour recognition) with the goal of providing a more comprehensive authentication information base on top of which we run the distributed authentication algorithm by the trust committee. Under this perspective, as for the MFA case, the achieved security is certainly at least equal to the sum of the standalone authentication systems (please refer to [26] for a more comprehensive study on MFA). As shown in Table 1, the key elements of the proposed solution are (i) the lack of a single point of failure (SPOF), (ii) the ability to run authentication algorithms on an arbitrarily long history stored in the authentication information base (AIB), and (iii) the decoupling from the collection of user information in the AIB, and the authentication algorithms. As for the lack of SPOF, we achieved this feature by introducing the Blockchain, which, through its consensus protocol, enforces a $k - over - n$ protection against server information tampering. The trusted committee enforces a distributed decision mechanism with similar propriety. The availability of an arbitrary long history is a straightforward consequence of such a technology choice. Finally, we decoupled the authentication information base from the authentication algorithm, constructing a common system and allowing different applications with different security requirements to run different algorithms on the same information base.

Table 1. Comparison of different authentication approaches.

Approach	SPOF	History Length	Auth Information Base and Auth Method
2FA	yes	2	coupled/binary
MFA [26]	yes	limited (e.g., 3)	coupled/binary
Federated identity for IoT [27]	yes	1	coupled/binary
Blockchain-based approach [15,28]	no	N/A	coupled/binary
SecurePath	no	arbitrarily long	decoupled/independent

6.3. Threat Model

The presented solution offers protection against the following attack model:

- **Malicious sensors**: Most of the current IoT devices can be easily tampered or tricked to emit incorrect information. This is the case of smart keys [29], voice recognition software [30], face recognition software [31], and location system [32]. Can we construct a trust model from many semi-trusted sources of information? Our rationale is that tampering/tricking many different devices is more difficult than attacking a single one, which is also the basic idea behind multi-factor authentication. In our system, we do not require devices to be trusted but to communicate non-reputable information in the form of certified data, which are conveyed in an immutable data store. Information can also be co-certified (using multi-signature) so that many different devices can agree on the same information (e.g., a user is in a given room).
- **Malicious data store**: Even if information by sensors is correct, there is always the possibility that the data on the receiving server can be manipulated. For this reason, we resort to Blockchain data streams (detailed in Section 3.2, which prevents such possibility by using a decentralised data store offering protection against data tampering.
- **Malicious authentication software**: Sensed data must be processed in order to determine where or not a user is authenticated to a system. We do this by using a trust committee (explained in Section 3.4), which is a set of N agents sharing the same logic and operating on the Blockchain.

7. Conclusions

Indoor localisation systems and the pervasive presence of IoT devices may provide continuous authentication schemes in smart spaces. Doors automatically unlock in front of users, PCs seamlessly log on to the intranet when users sit at their desks, and the room temperature can be dynamically reset as per the user′s preferences—these are a few examples of a broader set of newly enabled service possibilities. In this work, we presented a distributed architecture able to change the way we experience a smart space. All IoT interactions are exploited to provide a continuous authentication system with a greater level of security, ensured by chaining a series of challenges with spatial and temporal constraints. The presented system, currently under US patent, will be experimented with for identity management in smart spaces.

Author Contributions: Conceptualization, A.S., L.B. and P.L.; software C.P. and P.L.; methodology: L.B., P.L. and C.P.; investigation, L.B., P.L. and C.P.; writing—original draft, L.B. and P.L.; writing—review and editing, L.B. and P.L.; project administration, L.B.; supervision, A.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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

References

1. Perera, C.; Zaslavsky, A.; Christen, P.; Georgakopoulos, D. Context aware computing for the internet of things: A survey. *IEEE Commun. Surv. Tutor.* **2013**, *16*, 414–454. [CrossRef]
2. Michler, F.; Deniz, H.; Lurz, F.; Weigel, R.; Koelpin, A. Performance Analysis of an Ultra Wideband Transceiver for Real-Time Localization. In Proceedings of the 2018 48th European Microwave Conference (EuMC), Madrid, Spain, 23–27 September 2018; pp. 1141–1144.
3. Chin, W.H.; Fan, Z.; Haines, R. Emerging technologies and research challenges for 5G wireless networks. *IEEE Wirel. Commun.* **2014**, *21*, 106–112. [CrossRef]
4. Ross, A.; Jain, A. Information fusion in biometrics. *Pattern Recognit. Lett.* **2003**, *24*, 2115–2125. [CrossRef]
5. Sitová, Z.; Šeděnka, J.; Yang, Q.; Peng, G.; Zhou, G.; Gasti, P.; Balagani, K.S. HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 877–892. [CrossRef]
6. Zhang, F.; Kondoro, A.; Muftic, S. Location-Based Authentication and Authorization Using Smart Phones. In Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, UK, 25–27 June 2012; pp. 1285–1292. [CrossRef]

7. Stajano, F. Pico: No more passwords! In Proceedings of the International Workshop on Security Protocols, Cambridge, UK, 28–30 March 2011; Springer: Berlin/Heidelberg, Germany, 2011.
8. Riva, O.; Qin, C.; Strauss, K.; Lymberopoulos, D. Progressive authentication: Deciding when to authenticate on mobile phones. Presented at part of the 21st USENIX Security Symposium (USENIX Security 12), Bellevue, WA, USA, 5–10 August 2012; pp. 301–316.
9. 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, Los Angeles, CA, USA, 5–9 December 2016; ACM: New York, NY, USA, 2016; pp. 251–264.
10. Arias-Cabarcos, P.; Almenarez, F.; Trapero, R.; Diaz-Sanchez, D.; Marin, A. Blended identity: Pervasive IdM for continuous authentication. *IEEE Secur. Priv.* **2015**, *13*, 32–39. [CrossRef]
11. Shah, Y.; Choyi, V.; Subramanian, L. Multi-factor Authentication as a Service. In Proceedings of the 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, San Francisco, CA, USA, 30 March–3 April 2015; pp. 144–150. [CrossRef]
12. Ometov, A.; Petrov, V.; Bezzateev, S.; Andreev, S.; Koucheryavy, Y.; Gerla, M. Challenges of multi-factor authentication for securing advanced IoT applications. *IEEE Netw.* **2019**, *33*, 82–88. [CrossRef]
13. Maciej, B.; Kurkowski, M. Multifactor authentication protocol in a mobile environment. *IEEE Access* **2019**, *7*, 157185–157199. [CrossRef]
14. Dhillon, P.K.; Kalra, S. Multi-factor user authentication scheme for IoT-based healthcare services. *J. Reliab. Intell. Environ.* **2018**, *4*, 141–160. [CrossRef]
15. Dunphy, P.; Petitcolas, F.A. A first look at identity management schemes on the blockchain. *IEEE Secur. Priv.* **2018**, *16*, 20–29. [CrossRef]
16. Dai, H.N.; Zheng, Z.; Zhang, Y. Blockchain for Internet of Things: A survey. *IEEE Internet Things J.* **2019**, *6*, 8076–8094. [CrossRef]
17. Cui, Z.; Fei, X.; Zhang, S.; Cai, X.; Cao, Y.; Zhang, W.; Chen, J. A hybrid BlockChain-based identity authentication scheme for multi-WSN. *IEEE Trans. Serv. Comput.* **2020**, *13*, 241–251. [CrossRef]
18. Liang, W.; Fan, Y.; Li, K.C.; Zhang, D.; Gaudiot, J.L. Secure data storage and recovery in industrial blockchain network environments. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6543–6552. [CrossRef]
19. Stucchi, D.; Susella, R.; Fragneto, P.; Rossi, B. Secure and Effective Implementation of an IOTA Light Node using STM32. In Proceedings of the 2nd Workshop on Blockchain-Enabled Networked Sensor, New York, NY, USA, 10 November 2019; pp. 28–29.
20. Yue, Y.; Li, S.; Legg, P.; Li, F. Deep Learning-Based Security Behaviour Analysis in IoT Environments: A Survey. *Secur. Commun. Netw.* **2021**, *2021*, 8873195. [CrossRef]
21. Al Abdulwahid, A.; Clarke, N.; Stengel, I.; Furnell, S.; Reich, C. Continuous and transparent multimodal authentication: Reviewing the state of the art. *Clust. Comput.* **2016**, *19*, 455–474. [CrossRef]
22. Chuang, Y.H.; Lo, N.W.; Yang, C.Y.; Tang, S.W. A lightweight continuous authentication protocol for the Internet of Things. *Sensors* **2018**, *18*, 1104. [CrossRef] [PubMed]
23. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
24. Lenzini, G.; Bargh, M.S.; Hulsebosch, B. Trust-enhanced security in location-based adaptive authentication. *Electron. Notes Theor. Comput. Sci.* **2008**, *197*, 105–119. [CrossRef]
25. Lauridsen, M.; Krigslund, R.; Rohr, M.; Madueno, G. An empirical NB-IoT power consumption model for battery lifetime estimation. In Proceedings of the 2018 IEEE 87th Vehicular Technology Conference (VTC Spring), Porto, Portugal, 3–6 June 2018; pp. 1–5.
26. Ometov, A.; Bezzateev, S.; Mäkitalo, N.; Andreev, S.; Mikkonen, T.; Koucheryavy, Y. Multi-Factor Authentication: A Survey. *Cryptography* **2018**, *2*, 1. [CrossRef]
27. Fremantle, P.; Aziz, B. Cloud-based federated identity for the Internet of Things. *Ann. Telecommun.* **2018**, *73*, 415–427. [CrossRef]
28. Halpin, H. NEXTLEAP: Decentralizing Identity with Privacy for Secure Messaging. In Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, 29 August–1 September 2017; pp. 1–10.
29. Brocious, C. My arduino can beat up your hotel room lock. In Proceedings of the Black Hat USA, Las Vegas, NV, USA, 21–26 July 2012.
30. Roy, N.; Shen, S.; Hassanieh, H.; Choudhury, R.R. Inaudible voice commands: The long-range attack and defense. In Proceedings of the 15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18), Renton, WA, USA, 9–11 April 2018; pp. 547–560.
31. Ramachandra, R.; Busch, C. Presentation attack detection methods for face recognition systems: A comprehensive survey. *ACM Comput. Surv. CSUR* **2017**, *50*, 1–37. [CrossRef]
32. Cho, J.; Yu, J.; Oh, S.; Ryoo, J.; Song, J.; Kim, H. Wrong siren! A location spoofing attack on indoor positioning systems: The starbucks case study. *IEEE Commun. Mag.* **2017**, *55*, 132–137. [CrossRef]