applied sciences

MDPI

Article

Personalized Context-Aware Authentication Protocols in IoT

Radosław Bułat and Marek R. Ogiela *

Cryptography and Cognitive Informatics Laboratory, AGH University of Science and Technology,
30-059 Krakow, Poland
* Correspondence: mogiela@agh.edu.pl

Featured Application: Expected applications of the presented solutions—real-time context- and environment-aware user authentication—are ready for use in IoT environments (with low computing power but high sensor availability).

Abstract: The IoT is a specific type of network with its own communication challenges. There are a multitude of low-power devices monitoring the environment. Thus, the need for authentication may be addressed by many available sensors but should be performed on the fly and use the personal characteristics of the device's owner. Thus, a review and a study of the available authentication methods were performed for use in such a context, and as a result, a preliminary algorithm was proposed as a solution. The algorithm utilizes a variety of independent factors, including the user's personal characteristics, knowledge, the context in which the authentication is taking place, and the use of steganography, to authenticate users in the dispersed environment. This algorithm encodes all of these factors into a single data vector, which is then used to verify the user's identity or as a digital signature. Using this personalized context-aware protocol, it is possible to increase the reliability of authentication, given the emphasis on usability in low-computing-power but highly sensor-infused environments and devices. Although more testing is needed to optimize it as an industry solution, personalized protocols seem to have a future in the IoT world.

Keywords: IoT; personalized algorithms; authentication; cryptography

check for updates

Citation: Bułat, R.; Ogiela, M.R. Personalized Context-Aware Authentication Protocols in IoT. *Appl. Sci.* **2023**, *13*, 4216. https://doi.org/10.3390/app13074216

Academic Editor: Giacomo Fiumara

Received: 20 February 2023
Revised: 20 March 2023
Accepted: 21 March 2023
Published: 27 March 2023

1. Introduction

As society has become more interconnected in the Internet age and more and more of the processes of our daily lives are now automated, streamed, or dependent on the assistance of connected machines, user identification issues are becoming more common. Every device now needs some means of recognition of its administrators and users. As people are surrounded by machines or even their own personal mini-networks, often with minimal computing power, there is a risk of granting privileges or services to people who are not supposed to access them or, even worse, are leaking the (often sensitive) personal data to a third party or an external server or service. The consequences of such a data leak can be tragic and are most often irreversible (as our personalized devices hold a lot of PII (personally identifiable information), medical information (i.e., smartwatches), or credit card data (for e-commerce payments)). Such security issues are heavily regulated by ubiquitous laws and security standards (GDPR, HIPAA, and PCI-DSS, to name just a few), which enforce a high level of expected security for such devices and communications. As of today, there are three main avenues to authenticate one's identity [1].

The first is the knowledge-based method—asking for "something you know". These methods usually ask for a password, personal information, a PIN (personal identification number), or other information known (supposedly only) to the user. This does not guarantee successful authentication, as the method is not without the inherent risk of sharing the password/knowledge with a third party; stealing the password; or using social engineering, threats, or coercion (so-called rubber-hose cryptography) to mask a malicious actor as the authenticated individual [2].

The second method, unlike knowledge, is more physical; it works on a "something you have" basis, which can be a tangible physical object (such as a token, fob, or key card) or a digital asset (such as a digital certificate). Mobile phones, if uniquely bound to one user, can also be used to provide such means and might be an excellent example of an IoT device approach to security. Still, there are risks involved, similar to the above case; a token, although harder to spoof or to share, can still be stolen, which makes the whole setup fail.

The third method, personal protocol, unlike all the above, is not something separate from the individual being authenticated that could be "detached" and used by another individual. It is "something you are", which includes biometrics (a person's physical characteristics, such as a fingerprint or retinal scan) as well as other unique characteristics (typing cadence, gait, subconscious movements or twitches, etc.) It can be freely combined with any other method (e.g., typing the correct password with the correct rhythm that is specific to the rights holder) and could be difficult, if not nigh impossible, for an attacker to replicate. The anticipated risk lies in the refinement of the system. Criteria that are too stringent could lead to a high FRR (false rejection rate—a rejection of access to an individual who should be admitted), as even the rightful owner can sometimes change his habits, especially under duress (the inability to provide access during, for example, a hostage situation, might be dangerous). On the other hand, criteria that are too loose (for user accessibility) can make the system vulnerable to attacks, raising the FAR (false acceptance rate—accepting a user who is similar to the authorized one but should not be admitted) and defeating the whole purpose of the system. Moreover, as mentioned above, there has to be a strong consideration of the implications of storing (often sensitive) medical or personal data (used in biometrics) in the system's database. Finally, if we consider the practical applications, many of the devices that make up the Internet of Things (IoT) cannot handle the computing power needed for the complex calculations or advanced image recognition needed for some of these methods [3].

In the following sections:

- We describe the most popular personal characteristics and methods that could be considered in the development of advanced security protocols as well as judge their usability in the IoT context.
- We propose our own algorithms for advanced IoT authentication and message encryption:
    - For a single device.
    - For a small network of IoT devices.
    - For personalized communication security.
    - For a quick session CAPTCHA (completely automated public Turing test to tell computers and humans apart) check.
- We discuss the preliminary results and provide a basis for further studies.

2. Materials and Methods

As has been reviewed in preliminary studies, the methods that have already been used and proven/disproven to work fall into three main categories (with prominent examples below):

- Biometrics;

These include fingerprints, retinal patterns, and iris recognition [4,5]. All of these are based on the proven fact of the uniqueness of the characteristics being checked [6]. Retina checks have not proven to be usable in the IoT world, mainly due to the invasiveness of the procedure and the need for specialized scanners [7]. However, fingerprint sensors are currently widely used in the majority of more sophisticated devices (smartphones), and iris recognition, although more complicated, can still be achieved using modern cameras, given a properly lit environment [8]. Both of those methods require access to sensitive data and dedicated but readily available sensors.

- Neuroscience patterns;

These include subconsciously imprinted movements (trainable reflexes) or emotions (mental states). Both, although usable in IoT, have proven to be too specialized or challenging to use to be widespread. The first method requires a lot of training for the subjects as well as requires constant repetition to be usable [9], and the second one requires too much specialized equipment (EEG (electroencephalograph) scanners or electrodermal activity measuring equipment) and still can only be used in conjunction with another method, as it does not guarantee the uniqueness of a subject [10].

- Personal characteristics and habits.

These include typing cadence, eye movements, and sitting posture (with ECG (electrocardiograph) tracking). The latter, although tested and used in automated cars to secure the ignition system and recognize the driver, still requires a lot of specialized sensors and might be too cumbersome for widespread usage in the general IoT environment [11]. On the other hand, both typing cadence (during password or PIN checking) [12] and eye movement tracking have proven to be helpful, with a minimal surcharge of added computations to the standard authentication methods. Of these two methods, eye movement tracking can be particularly interesting, as it is based on reflexes that are trained with everyday usage and could be based on pattern/picture recognition by an authenticated subject [13].

Based on these categories [14] and the authors' work [15], a fourth category was proposed:

- Cognitive cryptography.

Due to the above methods, with some exceptions being too cumbersome or invasive, there is a need for methods that would need no more specialized equipment than what is already provided and could take advantage of the internal characteristics of an individual (which makes it closest to category three above). The main difference would be the awareness of the context of the authenticated person (whereabouts, daily routine, prerecorded habits, etc.) and the usage of the sensors that are available with the devices present on hand (be it a fingerprint reader, camera, a personal NAS (network-attached storage), a GPS (global positioning system), or a personal fitness band). All of these can be used to provide a digital footprint of their owner and authenticate based on already provided information, even if the data can be incomplete (due to a lack of proper sensors, bandwidth, processing power, or even WAN (wide area network) connectivity) [16].

The results of the comparative study can be seen below (Table 1) [15].

Table 1. Comparison of features for selected personal patterns and their usefulness.

Method	Sensors Accessibility for IoT	Minimal Computational Power	Contactless	Uniqueness Guarantee	Privacy Assured	Rating	Commentary
Fingerprints	1	1	0	1	0	3	Ubiquitous and unique, but uses biomedical data
Retina	0	0	0	1	0	1	Invasive and costly
Iris	1	0	1	1	0	3	Easy to implement but depends on lighting
Emotions/EEG	0	0	0	0	1	1	Hard to implement and maintain
Imprinted neural patterns	0	1	0	0	1	2	Needs training
Sitting posture	0	0	0	0	1	1	Specialized for cars
Typing cadence	1	1	0	0	1	3	Easy to implement, has a margin of error
Eye movement	1	1	1	0	0.5	3..5	Easy to implement, may access private data
Cognitive cryptography	1	1	1	1	0.5	4.5	A step above eye recognition, may still access private data

As can be seen in the above results, the most considerable risk, in this case, is personal privacy. A lot of the algorithm's strengths and weaknesses depend on the dataset of an individual, which might include just general data or operate on his personal history and biomedical scans (e.g., fitness tracker records) on as deep a level as there is consent to use. Thus, it has been rated as +/− [17].

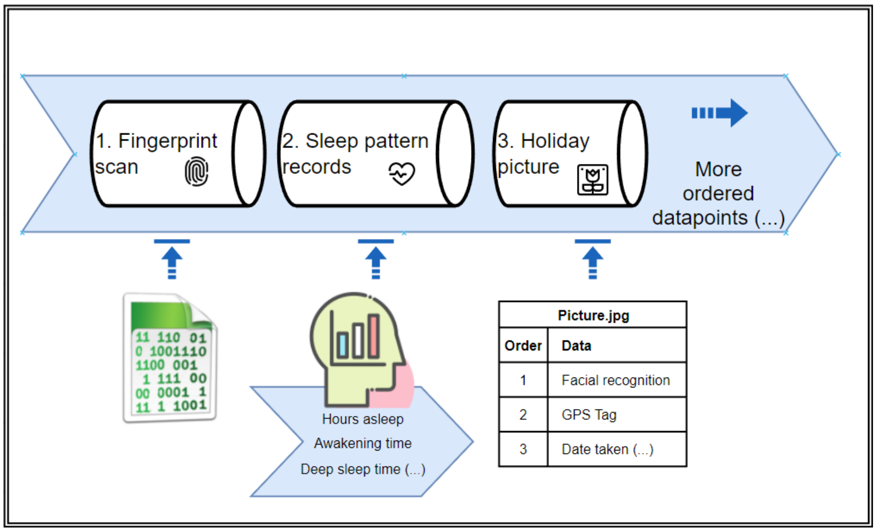
Given the nature of the context-aware algorithm, the data had to be carefully selected and curated. Thus, for the initial data vector usage, the following were considered:

- Fingerprints are one of the most ubiquitous forms of IoT access control. Sensors are widely used.
- Iris recognition is less popular but is still easy to use with facial and image recognition.
- Face recognition (see above) is an important part of biometrics. It does not guarantee uniqueness but needs to provide context, i.e., for user photos.
- Voice recognition is certainly not unique but is readily available and easy to capture and process on the fly. It is effective when paired with other methods [18].
- Speech patterns go hand in hand with voice recognition, giving context to a voice sample.
- Typing cadence is similar to speech patterns but is the equivalent for devices with keyboards.
- GPS data are only usable for providing user context but are readily available in a wide range of devices.
- Sleep patterns and ECG data are available from IoT fitness and health devices. They are classified as confidential health data.
- Scanned written signatures (or other handwriting samples) are used for context purposes.
- Social media data (freely available) are used by devices with social media access, using only publicly available information (freely shared by the authenticated person for public use).
- Social media data (with the individual's consent)—usage of private social media data and history, acknowledged and permitted by the device owner.
- Device usage history (i.e., browser history, time of access, etc., also needs consent) includes non-social data from web activity tracking engines or the device itself.
- Personal photos and media are highly confidential and require sign-off from the individual in question, but they are the best material for context generation. Ideally, there is a locally stored archive in the local network (i.e., an NAS connected to the smart home system) that consists of a collection of user data and his 'digital footprint'.

As can be seen, the data that can be used for authentication purposes form a vast spectrum. There are at least two caveats: in the case of private data, all the waivers or legal agreements (EULAs—end-user license agreements) have to be read and signed by the individual, and the appropriate standards of storing such data have to be observed as per the local regulations. In addition, as can be seen, many of the data points mentioned above can, and undoubtedly will, be spoofed or deep-faked (i.e., voice, facial recognition, or GPS coordinates). The proposed algorithm thus has to take this into account and always use an optimal set of data from different sensors to differentiate the input channels and make spoofing all of them at once an improbable occurrence. To summarize, a local network of the user, made from many different IoT devices, will share their sensor readings to provide the user with a personal digital portrait, including his or her characteristics, quirks, history, stored files, and every other bit of information that could be gleaned from these devices inputs, and this digital 'persona' will be used as a contextual model to compare any login attempt to the system with already known or predicted patterns to determine if the identity of the entrant matches any known 'persona' [19]. A cognitive personal recognition algorithm (CPRA) is thus proposed.

3. Results

As a result of all of the above state-of-the-art analysis and the preliminary queries into cognitive cryptography, a concept of a data vector of digital footprints was proposed. All of the mentioned datatypes can be joined into a structured data stream, with the possibility of addressing any part of it to access the data stored within, denoting the datatype and size of the block [20]. Thus, a sequence can be generated that is partially accessible to all of the devices in the personal network and dependent on their computing power and the ability to work on a specific data cell. The order and content of the sequence are personalized to the individual and depend on the most ubiquitous datatype, the consent given, and the devices available. An example vector can be seen in Figure 1. Every potential characteristic that can be used during the authentication process is assigned an address.



Picture.jpg	
Order	Data
1	Facial recognition
2	GPS Tag
3	Date taken (...)

Figure 1. An example of the data vector order.

The matrix structure is then populated to the IoT devices that are expected to be able to authenticate the individual. Every device marks the parts of the structure that are able to be processed locally by the device according to its hardware and sensor specifications, e.g., does it have a fingerprint scanner, a GPS, a camera, or local photo storage? Such information is held by the device as its local authentication ability profile (LAAP).

It also has to be noted that every device in the proposed algorithms only has access to its own sensor output/data storage and data that can be freely accessed through internet connectivity (in the case of social media). Thus, there is no centralized database (which would defeat the main advantage of IoT) for the data about an individual, and every device uses its own security methods to protect the data at rest (provided by the vendor). No personal data are sent over an unsecured network. Only random fragments of the datastream (Figure 1), challenge results, or hashes are to be used as data in transit.

3.1. *Basic Challenge–Response Algorithm with Masking—Basic CPRA*

The basic authentication procedure (proposed in this paper as the first of four algorithms —basic CPRA) is based on standard challenge–response protocols of a single IoT device, which are provided by the vendor software and provide basic readings from a device's sensors.

Assuming that a device owner wants to make use of its functions that need authentication (and more security than a simple fingerprint or face recognition scan), the individual being challenged has to present a semi-random set of characteristics (with a preference for those available to the available sensors on the fly) chosen from the LAAP set described above (and thus possible to be interpreted by the device). The LAAP of the device is analyzed, the device constraints and the abilities contained within are then taken into consideration, and a variable set of them is chosen to be used in an upcoming query. Thus, the queried sensor set is weighted to use either at least one of the characteristics that guarantee uniqueness or, in the case of a lack thereof, a balanced set of different media inputs (e.g., elements of facial recognition and biometrics matching the subject, GPS coordinates close to the position of the programmed daily itinerary, the subject's typing cadence, an eye-tracking pattern along a set of pictures matching those stored in device memory, etc.). As can be seen, in some of the cases a single sensor can be chosen (such as a normal fingerprint scan), but there is no indication of this to the user.

The chosen sensors are then responsible to use their own software, drivers, and algorithms (embedded in the device) to provide all of the requested characteristics of the user being queried. During every authentication attempt, any fragment of the LAAP can be queried in a random order (in a manner similar to, for example, the masked passwords used in digital banking to avoid sharing the whole secret over a possibly overt channel) (see Figure 1). As stated earlier, the choice is semi-random. A random data fragment accessible to the sensors is taken, and if the set taken so far does not guarantee uniqueness or is inconclusive, another one is queried in a similar manner until the taken set guarantees uniqueness or at least the accepted FAR/FRR criteria. A continuous stream of data sent by the device sensors in response to a given authentication attempt is then unpacked and interpreted according to the stipulated challenge and the vector address stored in the device (for example, a challenge asks for a fourth item of the second segment of the data vector). All of the captured data are then compared to the characteristics already stored in the device by its own software or firmware (a fingerprint vault or a health device's internal measurement storage). If all of the requested tests come up positive (or a selected majority of them in the case of less stringent controls and a higher accepted FAR), the user is granted access according to the results of the individual challenges and the FAR/FRR calibration that was set during the user's enrollment into the system. A decision of acceptance or rejection is made.

Thus, to sum all of the above, a random unpredictable set of challenges is selected for the user to be tested based on various characteristics. The data fields being checked vary between subsequent attempts (to create different keys that needs to be provided each time), and the sum of the individual results is judged according to data that were already gathered about the user and his metrics.

As can be seen, the more sensors or contextual data being used, the higher the dependability of the whole algorithm, as even a failure or an inconclusive result for one of the trials (for example, due to poor lighting conditions) can, depending on the calibration, not be a deciding factor for a user rejection. On the other hand, spoofed deep-fake visuals and GPS coordinates hypothetically may not match the user's personal calendar for the day and his typing cadence, which might lead to a rejection, since the potential attacker does not have knowledge on how the data stream will be interpreted in this particular challenge (similar to a one-time pad).

3.2. Distributed Challenge–Response Algorithm with Masking—Distributed CPRA

As can be seen, for the algorithm described in Section 3.1 to be used successfully, a relatively large number of nodes in the LAAP have to be available. Using only one or two data points will negate the algorithm's ability to choose a meaningful contextual set and might not provide enough data to ensure uniqueness, thus reducing the system to using only the most basic and unvaried methods of authentication without context or added security. On the other hand, it does not take advantage of one of the most prominent IoT features—interconnectivity. In an environment with a large number of interconnected devices belonging to one IoT gateway, a cloud-like solution can be implemented as a distributed CPRA. In such a case, a gateway can store any connected device's LAAP profile, treating it as a set, and the sum of all of the LAAP sets available at a given moment defines the combined authentication ability profile (CAAP) that can be used with all the devices and sensors working simultaneously. Thus, as the authentication begins for any of the networked devices, an attempt is made to obtain the CAAP. If no connection or CAAP is available, the algorithm can only downgrade to use LAAP (see Section 3.1 above). With a successful handshake, however, the device might use CAAP as the basis for the algorithm, indexing the data streams and sensors it does not physically own and does not have the access/permissions to use. When the protocol is negotiated and the challenge determined, the authenticating device determines its own sensor input and pattern matching and sends a request to the gateway to fill in for the lacking challenges (Figure 2). The networked devices are then polled by the gateway as needed (according to their advertised LAAPs) to perform their own authentication procedures on the subject (again, using a subset of the available methods chosen by the original device and provided by the gateway) and then return the result. In this manner, the original device does not have access to any external sensors or data it might not be authorized to access (which minimizes the risk of an accidental compromise to an infected device) and only receives partial reading results to use in its own final verdict of passing or failing the login attempt. It has to be noted that, although the individual communication and results from intermediate devices might be subject to spoofing attacks, the algorithm's unpredictability in choosing the challenge scales with network size, as with an abundance of similar sensors, a random suitable device can be chosen, and the same challenge can be issued to be processed by more than one device (which might then take the form of either a majority or a unanimous vote on the tested characteristics between the obtained results) (Figure 3).

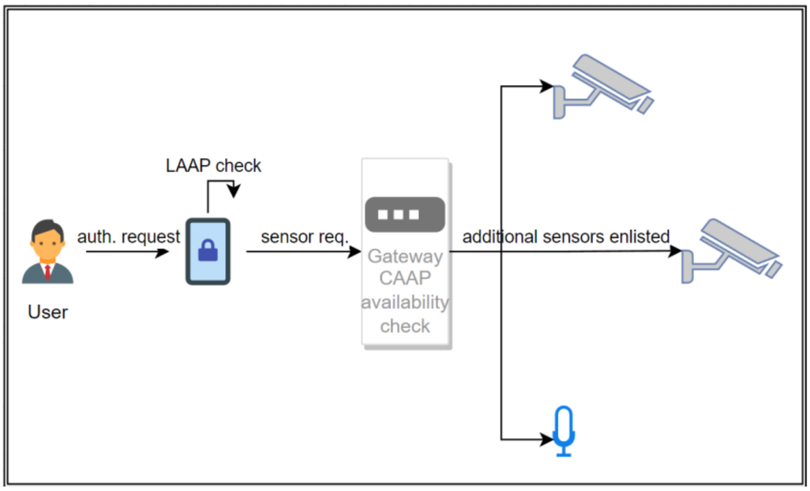


Figure 2. Distributed authentication challenge.

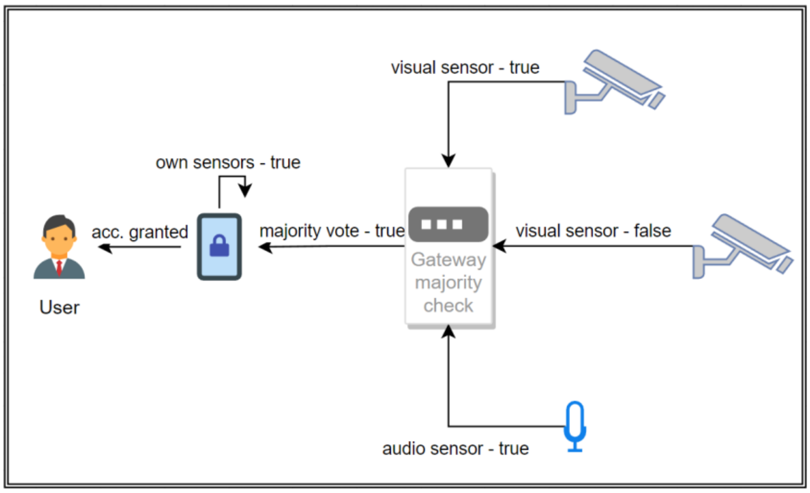


Figure 3. Distributed authentication response.

3.3. Digital Signature and Steganography—Steganographic CPRA [21,22]

Apart from the authentication of the user for the purpose of granting access, the addition of context from the identity vector might be used to sign the visual messages or files and data streams coming from an already authenticated individual, thus forming a steganographic CPRA. During a video capture session or a photo shoot, a random dataset is chosen from the LAAP/CAAP and communicated during the handshake protocol as a session key. Priority is given to the characteristics that are already measurable during the session (hand movements, involuntary tics, gestures, stutters, facial expressions, surroundings, GPS tags, etc.), similar to the semi-random vector procedure from Section 3.1. All of these individual qualities present in a picture or video being sent are quantified according to their values, given a sanity check of being in the acceptable range for the authenticated user (to weed out anomalous readings or unusual behavior), and merged into a digital stream that is ordered according to the negotiated protocol set (as shown on Figure 1, but only a subset is chosen). A hash of such a stream is made. The hash is then used as a mask for a steganography process. A secret message or a digital signature is encoded into the picture (by changing the least significant bits of pixels), only utilizing some of the pixels according to the mask and leaving the rest of the values untouched (see Figure 4 for a graphical representation). On the receiver end, a similar hash is computed from a received picture (according to the negotiated qualities), and the picture's steganography secret or watermark is then read (basically, the sent picture is used as an encoded message, and the calculated hash is used as a one-time pad). If the broadcast has been altered in any way during the transport (changing the biometrics, timestamps, coordinates, or voice or using AI-generated deep fakes), the quantities computed according to the key will deviate from the original material, and even a tiny deviation in these data will provide a fundamentally different hash value that cannot be successfully used as a pad to read the steganography part of the picture, as only a random sample of the bits will be pointed at, providing only white noise. In such a way, there are no personal data of the sender sent over (only what can already be inferred from a picture), and the data are tamper-resistant (even a slight change will provide only random noise and might destroy the secret part entirely). If the session key is compromised, the attacker might be able to read the signature/secret message, but would not be able to re-encode/change the message itself, as it would possess fundamentally different personal characteristics (Figure 4).

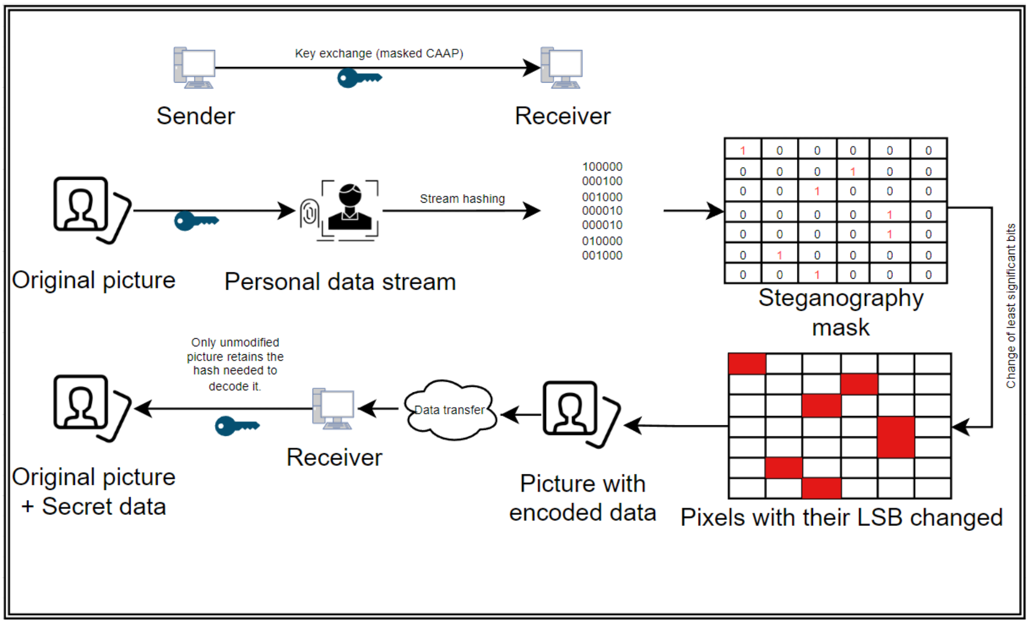


Figure 4. Secret message/watermark encoded with personal data.

3.4. Context Tracking—CPRA-CAPTCHA

As long as access to the digital footprint (public/authorized social media feeds of an individual) is granted to the device or a network of devices, additional methods of identity tracking can be instituted during the login procedure or occasional identity checks during prolonged service usage (to prevent session hijacking). Any device accessing this feed might use the following simple algorithm for CPRA-CAPTCHA (used as a safety method in addition to those of Sections 3.1–3.3):

- Input from the sensors is taken according to the chosen LAAP/CAAP. Only visual/audio/location sensors are used.
- The most current media feed of the person is accessed, and similar data are taken.
- A sanity check is performed. Are the location coordinates consistent with the latest ones (e.g., within traveling distance or half a world away)? If the location being shown is consistent with the subject's home/office/another already documented place, is the visual data feed consistent with previous data taken from the location in question? If the subject's calendar is accessible to the device, does the actual location match the itinerary?
- In cases of discrepancies, a CAPTCHA-like check might be applied to allow the continued use of the device. The check can be performed again using some of the subject's stored data, making the subject pick pictures known to him or made by him from a random batch. It can include a location-based check, where the pictures show nearby locations that the subject has visited, or a knowledge-based check, where a set of images connected to the subject's vocation or people they interact with on a daily basis are shown to pick from. The actual check can be performed without much interaction by using eye tracking (if permitted by the device) [13].

As can be seen, this method does not guarantee uniqueness and can only work as intended if given access to a substantial amount of the subject's data, which may or may not be viewed favorably by the subject. As such, it could only be used as a supporting method to ensure that the device has not been stolen and the session has not been hijacked.

4. Discussion

The study so far has established a few points that could serve as a basis for further research:

- As has been seen during the review phase, there are many methods of varying usefulness available to authenticate a person only by their individual characteristics rather than their knowledge. A lot of these are not context-sensitive and only use a singular biometric scan to assure the identification. Thus, they remain susceptible to mimicking or session hijacking.
- At the same time, most people using any kind of networked personal device during their daily routine produce a tremendous amount of personal data from various sources. Some of these data are publicly available, and some have to be protected due to privacy reasons.
- IoT devices used by any individual have a wide array of sensors that are mainly dedicated to the primary function of the device. In more significant numbers and when used simultaneously, they are able to build a digital representation of the owner's behaviors and routines.
- Given all of the above, our research shows proof-of-concept methods and algorithms that could utilize the IoT's strengths and downplay its weaknesses, relying on distributed and already available data.

As such, the proposed methods seem to fill a market niche, enforcing IoT devices' connectivity and functionality while downplaying their limited computational power by distributing the load and authentication tasks between many devices. Care is being given not to use or send personalized data out of the device that collected it (with the owner's consent). Further study of the method's effectiveness is still ongoing, and care is being given for it to remain ethical, safeguard privacy laws, and at the same time, secure individuals' data and communication by embracing their humanity and individuality.

Author Contributions: R.B.: Conceptualization, methodology, validation, formal analysis, investigation, writing—original draft, and visualization. M.R.O.: Conceptualization, methodology, validation, writing—review and editing, and supervision. All authors have read and agreed to the published version of the manuscript.

Funding: This work was partially supported by the funds of the Polish Ministry of Education and Science assigned to AGH University of Science and Technology. This research project was supported by the program "Excellence initiative—research university" of AGH University of Science and Technology.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

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

References

1. Menezes, A.J.; Vanstone, S.A.; van Oorschot, P.C. *Handbook of Applied Cryptography*, 1st ed.; CRC Press, Inc.: Boca Raton, FL, USA, 1996.
2. Hadnagy, C. *Social Engineering: The Science of Human Hacking*, 2nd ed.; Wiley Publishing: Hoboken, NJ, USA, 2018.
3. Sfar, A.R.; Natalizio, E.; Challal, Y.; Chtourou, Z. A roadmap for security challenges in the Internet of Things. *Digit. Commun. Netw.* **2018**, *4*, 118–137. [CrossRef]
4. Fierrez, J.; Morales, A.; Vera-Rodriguez, R.; Camacho, D. Multiple classifiers in biometrics. Part 2: Trends and challenges. *Inf. Fus.* **2018**, *44*, 103–112. [CrossRef]
5. Traore, I.; Ahmed, E.A. *Continuous Authentication Using Biometrics*, 1st ed.; IGI Global: Hershey, PA, USA, 2012. [CrossRef]
6. Srihari, S.; Srinivasan, H.; Fang, G. Discriminability of fingerprints of twins. *J. Forensic Identif.* **2008**, *58*, 109.
7. Mazumdar, J.B. Retina based biometric authentication system: A review. *Int. J. Adv. Res. Comput. Sci.* **2018**, *9*, 711–718. [CrossRef]
8. Galbally, J.; Gomez-Barrero, M. A review of iris anti-spoofing. In Proceedings of the 2016 4th International Conference on Biometrics and Forensics (IWBF), Limassol, Cyprus, 3–4 March 2016; pp. 1–6. [CrossRef]
9. Bojinov, H.; Sanchez, D.; Reber, P.; Boneh, D.; Lincoln, P. Neuroscience meets cryptography. *Commun. ACM* **2014**, *57*, 110–118. [CrossRef]
10. Gupta, P.; Gao, D. Fighting Coercion Attacks in Key Generation Using Skin Conductance. In Proceedings of the 19th USENIX Conference on Security, Washington, DC, USA, 11–13 August 2010; p. 30.
11. Riener, A. Sitting Postures and Electrocardiograms. In *Continuous Authentication Using Biometrics*; IGI Global: Hershey, PA, USA, 2011; pp. 137–168. [CrossRef]
12. Panasiuk, P.; Saeed, K. A Modified Algorithm for User Identification by His Typing on the Keyboard. In *Image Processing and Communications Challenges 2, Choraś, R.S., Ed.*; Springer: Berlin/Heidelberg, Germany, 2010; Volume 84, pp. 113–120. [CrossRef]
13. Ogiela, M.R.; Ogiela, L. Eye Tracking Solutions in Cognitive CAPTCHA Authentication. In Proceedings of the 2020 12th International Conference on Computer and Automation Engineering, Sydney, NSW, Australia, 14–16 February 2020; pp. 173–176. [CrossRef]
14. Liang, Y.; Samtani, S.; Guo, B.; Yu, Z. Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective. *IEEE Internet Things J.* **2020**, *7*, 9128–9143. [CrossRef]
15. Bułat, R.; Ogiela, M.R. Comparison of Personal Security Protocols. In *Advanced Information Networking and Applications. AINA 2021*; Springer: Cham, Switzerland, 2021; pp. 672–678. [CrossRef]
16. Ogiela, M.R.; Ogiela, L. Cognitive Keys in Personalized Cryptography. In Proceedings of the 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), Taipei, Taiwan, 27–29 March 2017; pp. 1050–1054. [CrossRef]
17. Loukil, F.; Ghedira-Guegan, C.; Benharkat, A.N.; Boukadi, K.; Maamar, Z. Privacy-Aware in the IoT Applications: A Systematic Literature Review. In *International Conference on Cooperative Information Systems (CoopIS) 2017. Proceedings, Part. I. LNCS*; Springer: Cham, Switzerland, 2017; Volume 10573, pp. 552–569. [CrossRef]
18. Szlosarczyk, S.; Schulte, A. Voice Encrypted Recognition Authentication—VERA. In Proceedings of the 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, Cambridge, UK, 9–11 September 2015; pp. 270–274. [CrossRef]
19. Acien, A.; Morales, A.; Vera-Rodriguez, R.; Fierrez, J.; Tolosana, R. MultiLock. In Proceedings of the 1st International Workshop on Multimodal Understanding and Learning for Embodied Applications, Nice, France, 21–25 October 2019; pp. 53–59. [CrossRef]

20. Bułat, R.; Ogiela, M.R. Personalized Cryptographic Protocols—Obfuscation Technique Based on the Qualities of the Individual. In *Advances in Networked-Based Information Systems. NBiS 2021*; Springer: Cham, Switzerland, 2022; pp. 213–218. [CrossRef]
21. Ogiela, M.R.; Koptyra, K. False and multi-secret steganography in digital images. *Soft Comput.* **2015**, *19*, 3331–3339. [CrossRef]
22. Cox, I.; Miller, M.; Bloom, J.; Fridrich, J.; Kalker, T. *Digital Watermarking and Steganography*; Elsevier: Amsterdam, The Netherlands, 2008. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.