IoT-based Activities of Daily Living for Abnormal Behaviour Detection: Privacy Issues and Potential Countermeasures

Mustafa A. Mustafa, Alexandros Konios and Matias Garcia-Constantino

Abstract

Activities of daily living (ADL) systems have been playing an important role in assessing and monitoring the quality of life of elderly people for many years. With the recent advancement and integration of internet of things (IoT) devices within the ADL systems, the number and quality of services offered has increased significantly. One of these vital services is abnormal behaviour detection based on the data collected from IoT devices within smart homes. However, the IoT data collected could have enormous privacy implications on smart home users if the data is not handled properly. We address this issue by analysing a generic ADL system for abnormal behaviour detection, including its entities and their interactions. We highlight three major privacy issues: (i) identity privacy, (ii) data confidentiality, and (iii) metadata data leakage. These issues are particularly relevant to ADL systems and we propose potential countermeasures to tackle them. Finally, we sketch a privacy-preserving version of an example ADL system to demonstrate the effectiveness of our proposed countermeasures, before suggesting future research directions.

Introduction

Activities of daily living (ADL) refer to daily self-care activities of people such as feeding, bathing, dressing, grooming and cleaning. A person's (in)ability to perform ADL is often seen as a sign of their well-being [1]. This is particularly the case with elderly citizens or people with disabilities. Analysing various ADL of people is a promising approach for monitoring their well-being and general health status. Such analyses could help to detect unusual activities (abnormal behaviour) that could be an indicator of a progressive health issue taking place (e.g., dementia, osteoporosis, arthritis) or an occurrence of a hazardous incident (e.g., fall, burn, cut, food or smoke intoxication). In the latter case, acting timely could be of paramount importance for limiting the impact of such life-changing or even life-threatening incidents.

With technological advances on the internet of things (IoT) domain, smart environments (e.g., smart home) populated with a diverse set of IoT devices, rich on sensors, are becoming an integral part of our daily life, thus making the monitoring of ADL of people possible [2]. IoT devices can be placed within the environment and appliances of interest, hence generating valuable data that can be used in the detection and monitoring of ADL. Usually, such data is collected (via wireless connection) by a local node (gateway) and sent to a third-party service provider for data analysis. The results are then sent back to authorised users (e.g., the monitored users themselves or their close relatives). Existing solutions typically rely on cloud environments to perform the data analysis.

However, data collected from IoT devices could be very privacy-invasive as one, by analysing the data, can reconstruct all the activities performed by the users in the smart environment [3]. For example, one could infer exactly when a user is cooking, taking a bath, entering/exiting the smart environment, etc., which is extremely privacy-invasive. Existing solutions do not consider users' privacy as their system model rely on a central entity that collects, and has access to, all the IoT data generated within the smart environment.

Hence, privacy-enhancing solutions are needed for monitoring and analysing ADL; solutions where central entities do not have access to all the raw IoT data, but only to a modified version of the data (e.g., masked, encrypted), which is still useful for ADL monitoring, while at the same time does not pose privacy risk to users.

The contributions of this article are threefold:

- It analyses a generic system for monitoring and detecting ADL to highlight three major privacy issues in such systems: (i) identity privacy, (ii) data confidentiality, and (iii) metadata data leakage.
- It suggests countermeasures that can be applied to address these privacy issues.

- It shows how privacy-enhancing techniques can be applied to a state-of-the-art ADL solution to demonstrate that detecting abnormal behaviour in ADL can be achieved in a privacy-preserving manner.

The remaining part of this article is organised as follows. We present the related work in the area of ADL before analysing a generic system model of a typical ADL monitoring system. We discuss the privacy issues in such systems and suggest countermeasures to address them. Finally, we present a use-case of a privacy-preserving ADL system and suggest future research directions.

Activity of Daily Living Analysis

IoT sensor data collected in smart environments have already been used for activity recognition in ADL to detect and predict abnormal behaviour. For example, the model presented in [4] collects IoT sensor data from house appliances, generates sensor activity patterns and then classifies these patterns as regular and irregular, thus predicting the behaviour of the elderly occupants of the house. The model proposed in [5] collects data from home sensors (e.g., movement and door entry sensors) and analyses these data using neural networks to predict abnormal behaviour of elderly occupants suffering from dementia.

A probabilistic spatio-temporal model is used in [6]. The model collects data from motion, door and pressure sensors to build the 'normal' daily behaviour of occupants. It then classifies as 'abnormal' any behaviour that is considerably different from the built 'normal' behaviour. Petri nets are utilised in [7] to model three ADL: preparing tea, coffee and pasta. The model flags up abnormal behaviour if any of these ADL is incomplete. A unified approach for detecting (ab)normal behaviour based on the analysis of ADL is proposed in [8].

A probabilistic approach based on cumulative distribution function for the temporal analysis of ADL is proposed in [9]. The authors demonstrate that their methodology could be an efficient and effective way to classify a certain ADL as normal or abnormal behaviour based on its duration. The same approach is applied also to analyse ADL with respect to step sequences [10].

System Model and ADL Phases

Below we present a generic system model for ADL analysis (see Figure 1), including the system entities and an overview of the main ADL phases.

System model

Users are the people interacting with the smart environment, and whose ADL we want to detect and analyse. They could be grouped in two categories: *hosts* and *visitors*. Hosts (e.g., people who live there) regularly interact with the smart environment. Visitors occasionally interact with the smart environment, for example, people who visit the occupants of the smart environment.

Sensors are the sources of the IoT data collected and analysed for the purpose of ADL analyses. They can sense various types of (physiological) data and make this data available for analysis. There are two types of sensors: *environmental* and *wearable*. The former (cameras, locks, TVs, contact/dense sensors) are embedded to the environment (i.e., attached to various objects: door, kettle, mug), hence they are (relatively) static. On the other hand, wearable sensors (wristband, smart watches, smart clothes, smart phones) are attached to users (i.e., to their body or clothes) and typically measure movements and physiological values.

Gateway is a device located in the smart environment that collects IoT data from the sensors to (i) either analyse the data locally, or (ii) send the data to third-party service providers for further analyses.

Service providers (SPs) are third-party companies that collect and analyse IoT data to extract valuable information for beneficiaries.

Beneficiaries are the entities interested in the results of the IoT data analysis. One category of beneficiaries includes the users themselves and their close family members and relatives. Other categories include the medical staff (doctors, nurses), researchers and other third-party companies.

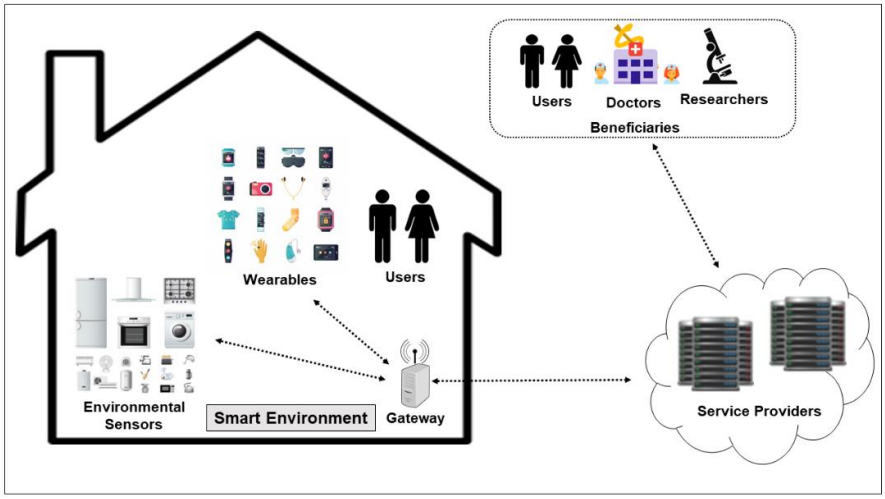

Figure 1: A generic system model for analysing ADLs in smart environments.

ADL analyses phases

Below we give an overview of the main phases of a typical ADL system (see Figure 2).

System setup is the initial phase during which the system is set up, that is environmental IoT sensors are connected to the gateway (and to each other). This phase usually takes place only once.

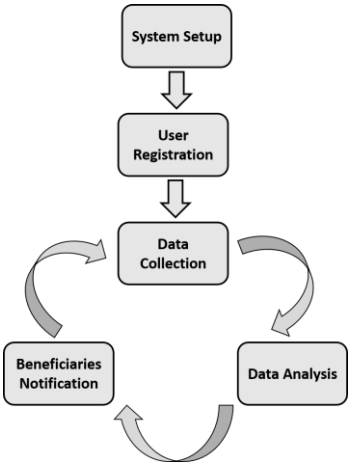

Figure 2: Overview of ADL phases in smart environments.

User registration is the phase when users register with SPs and their wearables/smart devices are connected and paired with the system. This phase usually takes place only for the host users, and only once per user. Visitors may not register with the system; they are treated as guest users.

Data collection is the phase when users interact with the smart environment while carrying on with their daily activities. During this phase, various sensor data are collected and sent to the gateway or the SPs for data analysis.

Data analysis is the phase when the collected sensor data are analysed to identify any ADL, and then extract useful information such as detection of abnormal behaviour.

Beneficiary notification is the phase when the outcome of the analysis is sent to beneficiaries. The outcome can be continuously fed to (some of) the beneficiaries or only specific results under specific conditions could be made available (e.g., only if abnormal behaviour has been detected).

Privacy Issues in ADL Systems and Potential Countermeasures

ADL systems could be beneficial for monitoring the well-being of (elderly) people to detect any abnormal behaviour and act on a timely manner. However, monitoring people at all times pose a serious threat to their privacy. We discuss several privacy issues that arise from the ADL analysis and propose potential countermeasures to address these issues.

Identity privacy

Identity privacy in the context of ADL systems relates to the protection of the identity of the users whose activities are being monitored. If the identity of the users is known to the SPs who have access to the IoT sensor data, the SPs can correlate the data (and any identified medical conditions) to specific users, which may not be strictly necessary. In addition, they could also share some of the findings with unauthorised third parties, which is illegal without explicit user consent. The findings might also be obtained by criminals if the SPs' databases are breached.

A potential solution to this threat is the use of *pseudonyms* instead of user identities, so that the link between the users' data and identity is hidden. Frequent changes of these pseudonyms are recommended in order to reduce the risk of an external attacker linking the compromised IoT sensor data to a single user. Note that the use of pseudonyms is usually not sufficient, especially if there is a need to protect users' identity against malicious SPs. In such situations, the use of pseudonyms combined with *group signatures* is recommended.

Group signatures allow a verifier (in this case SPs) to verify that a user belongs to a group of legitimate users without learning the identity of the user. However, the size of the group would result in implications with respect to the privacy protection of users. If a group contains only a single and/or few members, the SPs would be able to deanonymize the group members. Advanced cryptographic techniques such as *anonymous credentials* and *zero-knowledge proofs* could also be used. However, these techniques might not be suitable for resource-constrained IoT devices.

Another promising line of research is called frictionless (a.k.a. seamless or collaborative) authentication that allows users to authenticate themselves towards SPs by just using wearables with minimum human interaction [11-13]. The main idea behind frictionless authentication is to deploy multiple user devices (e.g., smartphone, smartwatch, wristband) and use them as multiple collaborating provers towards a verifier in a challenge-response protocol. The signing key of a user is split into shares and each user device stores a single share. The advantage of this type of authentication is that the signing key is never stored on a single device nor is reconstructed. Instead, the user devices use their shares of the key to generate shares of the signature, which are then combined to reconstruct the user signature on the challenge.

To mitigate the threat of one or more user devices being lost or stolen, as well as to accommodate a dynamic set of wearables (a user may not always carry the same set of wearables), *threshold cryptography* could be used. Threshold cryptography protects a secret by sharing it amongst a number of entities in such a way that only a subset of minimal size, namely a threshold *t* (out of, say *n*, *n* > *t*), can recover the secret. No information about the secret can be learnt from *t* - *1* or less shares. This allows user authentication as long as at least *t* shares (i.e., user devices) are present. In case a new device is added, or existing devices are lost or damaged, the user signing key can be re-shared without being reconstructed.

Furthermore, if some of the user devices do not have a sufficient size of secure storage, they can instead generate their respective share on the fly with the help of fuzzy extractors using biometric data of the user. Figure 3 shows an overview of such authentication protocols.

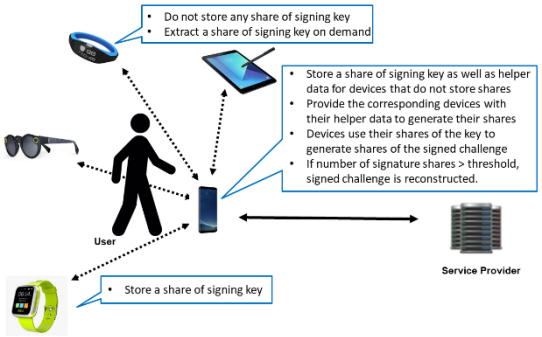

Figure 3: Overview of frictionless authentication protocol.

If users do not possess wearable devices, they can use their smart phones (which would hold a copy of their signing key) to authenticate themselves to the SPs (via the gateway). It is worth mentioning that the system would be able to authenticate only the host users who had been registered with the system beforehand. Visitors would be treated as guest users whose data could be gathered and analysed by comparing it to a global (average) user behaviour. If abnormal behaviour is detected, the system could then notify the host of the premise that there is an unusual behaviour occurring at their premises.

Furthermore, inevitably, in some cases, some SPs, for example the ISP, will know the identity of the users. In these cases, it is important to apply the principle of separation of concerns, which advocates dividing the access privileges of SPs. In this particular case, if the ISP has access to user identities, it is important to block its access to users' sensitive data such as IoT sensor data.

Data confidentiality

Data collected from smart environments contain user-specific information. If an unauthorised entity has access to these data, it can infer user sensitive information such as who does what at what time and how often. Such an access could be extremely privacy-intrusive; thus, information needs to be protected. As most smart environments use wireless networks to send data, protecting the confidentiality of data becomes of a paramount importance, especially in ADL, as the collected sensor data might be directly linkable to some medical conditions of users.

The obvious countermeasure is the use of encryption. However, as IoT devices are usually resource-constrained, the use of *lightweight encryption schemes* designed for deployment at IoT devices is recommended. To prevent the intermediate nodes in the system (e.g., gateway) to be a potential point of leak, *end-to-end encryption* should be deployed. In such schemes, only the sender (i.e., IoT device) and the receiver (e.g., medical doctor) will have access to the data.

Depending on the threat model used, end-to-end encryption may not be enough to protect users' privacy. For example, in some scenarios the SPs that analyse the sensor data might be seen as an adversary (an entity with malicious intentions or behaviour), hence even they should not have access to the raw IoT data. The obvious solution is to use local processing, that is ADL monitoring and abnormal behaviour detection takes place within the premises of the smart environment. In other words, the prediction models of the SPs run on local devices – data are collected, processed and analysed locally without leaving the physical boundaries of the smart environment. Assuming that access to the smart environment is restricted only to legitimate users, the IoT data would be protected. The role of the SP in this case would be simply to allow their prediction model to run on local devices and verify the correctness of the result produced by the model without having access to the IoT data, nor the results.

However, some prediction models might need to be run on cloud environments. In such cases, the IoT data also need to be protected from cloud providers. The data should be modified such that secure computations can be performed on the data. There are two main cryptographic techniques that allow secure computation: *homomorphic encryption* and *secure multiparty computation*. Both techniques allow various operations to be performed on encrypted data. IoT devices could play the role of data providers that pre-process the data and then let the computational parties (i.e., SPs, gateway or cloud providers) run the prediction model on the encrypted data.

Metadata data leakage

Metadata is all the side data that provides extra information about the core (primary) data. For example, the time/frequency of data generation, communication and processing is metadata, and it may leak sensitive information about the core data. In other words, hiding the content of the data may not be enough to protect users' privacy. For example, even if (i) pseudonyms, instead of user identity, are used, and (ii) the IoT sensor data are encrypted, attackers might still learn private information about users just by analysing the communication patterns within the smart environment and with the SPs. A potential countermeasure against this leakage is the use of padding, so that the communication patterns have constant parameters.

Privacy-enhancing ADL System

We present an overview of a simple yet effective probabilistic approach for temporal analysis of ADL [9] and demonstrate how this approach can be realised in a privacy-preserving manner.

Use-case: analysis of kitchen ADLs

Let us take the probabilistic approach for temporal analysis of ADL proposed by Garcia-Constantino et al. [9]. It aims to demonstrate that a relatively simple probabilistic approach could be very effective in classifying the execution of certain ADL as normal or abnormal behaviour based on the duration of these ADL.

Kitchen ADL

Two kitchen ADL (coffee and tea preparation) which a person can perform multiple times a day are investigated. In their experiment, volunteers perform any of these two ADL the way they prefer.

Table 1: Activities and Stages Duration (in seconds).

Vol. ID	Entering	Preparation	Drinking	Exiting	Total Time
1	5	144	670	21	840
2	44	110	481	21	656
…	…	…	…	…	…
29	56	84	356	20	516
30	8	170	759	4	941
Average	35.07	150.27	577.47	16.27	779.08
Standard Deviation	19.26	43.93	240.28	8.09	231.99

The only restrictions placed on the volunteers are as follows: (i) each participant prepares only one drink, (ii) coffee/tea is drunk at the table, and (iii) the cup is placed in the sink. They also follow a concrete scenario: enter kitchen, prepare tea or coffee, sit at the table while drinking, leave the cup in the sink and exit the kitchen. For the ADL analysis, this scenario is broken down into four main stages: (i) enter kitchen, (ii) prepare a drink, (iii) drink, and (iv) exit kitchen. The aim is to associate the duration of each stage or of the entire ADL with potential abnormal behaviour. Abnormal behaviour is defined as a value (i.e., duration of stages) that deviates considerably from the average sample values and lies outside a predetermined value range that defines the spectrum of all users' behaviour.

Volunteers selection

For the experiments, 30 volunteers (16 males and 14 females) are recruited, the youngest and oldest being 22 and 43 years old, respectively. Two of them (one male and one female) are known to have a chronic medical condition. The experiments are conducted in the smart kitchen lab of the Smart Environments Research Group (SERG)[1] at Ulster University (see layout in Figure 4). Data from three types of sensors (contact, thermal and accelerometer) attached to the objects of interest (doors, cups, cupboards, tea/coffee/sugar/milk containers, refrigerator, worktop, table and sink) are collected by a sensor data platform called SensorCentral [14]. The contact sensors are represented in Figure 4 as rectangles. The colour codes in the legend indicate the objects to which these sensors are attached.

[1]https://www.ulster.ac.uk/research/institutes/computer-science/groups/smart-environments

The IoT sensor data are collected, pre-processed and analysed. The average and standard deviation of the durations are calculated to define the average time of execution per stage and the range under which a behaviour can be considered as normal for each stage and activity. The range given by the average value and the standard deviation denotes the durations that correspond to normal behaviour. Then, when the durations of the stages of each user's ADL activity are compared to this range, it was detected that on average the durations of the ADL of two volunteers fall outside the set range for normal behaviour - exactly the number of volunteers who have chronic medical conditions.

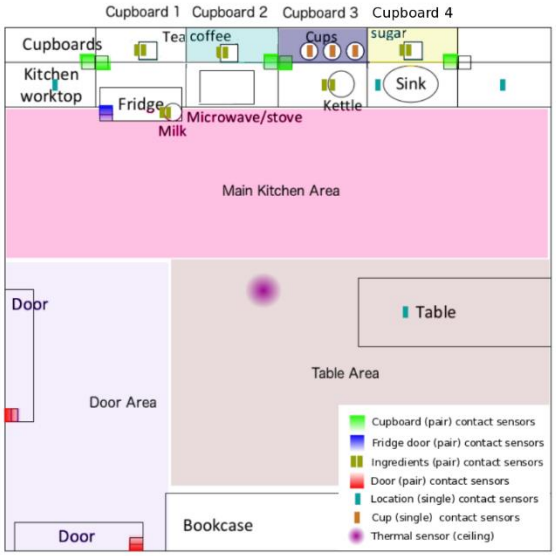

Figure 4: Smart kitchen layout at SERG.

Privacy-preserving Analysis of Kitchen ADL

Although the approach proposed in [9] accurately detects abnormal behaviour by analysing two

kitchen ADL, it uses a central entity, the SensorCentral platform, that has access to all the users' data. We propose ways to realise the same approach achieving the same level of accuracy in a more privacy-preserving manner, by applying some of the countermeasures discussed earlier.

Use multiple ADL session-specific pseudonyms per user

To address the user identity privacy issue, multiple session-specific pseudonyms per user should be used. The real identity should be used only when the user registers with the SP, and user-specific credentials are issued. To protect the user's privacy further, this identity can be kept local and only a static pseudonym can be shared with the SP. The SP then will know a specific user only by this static pseudonym, but never by the real identity. When users perform a specific ADL, they will need to authenticate. However, this authentication takes place within the smart environment, between the users and the gateway (details to follow).

For any communication between the user and the SP, the user employs an ADL session-specific pseudonym, so that the SP cannot link two sessions of the same user, and cannot determine whether any given two sessions have been completed by the same user. The link between the real identity and the session pseudonym should be revealed only to the authorised beneficiaries. In other words, even if the SP's analysis determines that the user's behaviour is abnormal, the SP should still not know the real identity of the user. If such detection happens, the SP should only reveal the session-specific pseudonym of the user to the beneficiaries. The beneficiaries then could use this session-specific pseudonym to identify the real identity of the user by communicating directly with the smart environment.

Use of group signatures

As mentioned above, each user should always authenticate to the system before the start of any ADL. This is necessary to link the outcome of the ADL analysis to that specific user. However, to protect users' identity privacy, a group signature scheme should be used when authenticating. Group signature schemes allow a member of the group (i.e., a user) to prove to the verifier (i.e., the SP) that she is a valid member of the group without revealing her real identity. Therefore, every time a user performs an ADL session, the IoT sensor data related to this session will be processed and analysed by the SP, as it comes with a proof that it belongs to a legitimate user, but without revealing the real identity of the user; a session-specific pseudonym is used instead. In addition, to enhance usability and convenience, the user could utilise the IoT sensor data coming from her wearables to perform the authentication in a frictionless way [13].

Use lightweight encryption schemes

To provide data confidentiality, all the communication between the IoT sensors and the gateway should be encrypted. Given that, most IoT sensors are resource-constrained devices, the encryption scheme used should be lightweight, specifically designed for use in the IoT domain.

Use local computation

To protect IoT sensor data from being leaked to the SP, all the data should be analysed locally, whenever this is feasible. In the approach proposed in [9], the operations are relatively simple consisting of (i) determining the durations of the kitchen ADL stages, (ii) calculating the average duration and standard deviation of these stages, thus determining the range of durations that define a normal behaviour, and (iii) checking whether the durations of the ADL stages of each user falls within the defined range. These computations are lightweight and could be performed at a local device that has more resources than a typical IoT device (e.g., the gateway or another user-owned trusted device). In other words, the IoT sensor data are processed locally; they never leave the physical borders of the smart environment. Note that this local device could recalculate and update the average ADL stage duration as well as standard deviation after each ADL session. Ideally, this should be done on a per user basis, so that the approach proposed can provide more accurate results. In addition, the system should be set such that it notifies the beneficiaries (and maybe the SP) only if abnormal user behaviour is detected. This way, as long as the user ADL are classified as expected, the SP will not know who has performed the ADL, at what time and for how long, hence further enhancing the privacy protection of users.

It is worth noting, however, that processing the data locally is only possible if the computations required for the data analysis are relatively simple (as in the approach proposed in [9]) or a device with relatively powerful computational capabilities (such as server or desktop PC) is available locally within the premises of the user.

In case the operations in the analysis stage are not possible to be performed locally due to the limited computation capabilities available, these operations can be outsourced to the SP's servers without revealing any IoT sensor data. This is possible due to the powerful properties of *homomorphic encryption*, as demonstrated by Preuveneers et al. [15], and *secure multiparty computation* schemes that allow computations to be performed on encrypted data. These techniques could also be deployed when using relatively simple machine learning techniques.

Use padding for constant communication patterns

To protect against metadata data leakage, the ADL system could be set such that it generates constant communication patterns. For example, the IoT sensors could be set to transmit their data at certain intervals of time, regardless if they have new measurements or not. This way, an eavesdropper will not be able to determine if the observed communication is due to ADL or redundant data. Note that, although these constant-time communication patterns provide extra protection for users' privacy, they come with additional overheads.

Another approach would be the IoT sensors to store all their data for a certain period of time (e.g., one day) and then send them in batches. This approach could be more efficient. However, it adds delays in the ADL system, which might have fatal consequences when acting timely is of paramount importance.

In summary, a combination of techniques (i.e., session-specific pseudonyms, group signatures, lightweight encryption scheme, local processing and padding) allows a design of a privacy-preserving system for analysis of ADLs.

Future research directions

We highlight some of the remaining challenges and possible future research directions.

Practical seamless authentication: Although frictionless authentication has seen some recent advancements, they still lack high accuracy and precision. Further research is needed to improve the process in terms of the false positive and negative rates. To be widely deployed, such authentication schemes should be more reliable.

Efficient secure computation: Techniques such as homomorphic encryption and secure multiparty computation are already, to a certain degree, practical and deployed in real-world applications. However, deploying them on resource-constrained IoT devices is still not possible. Further research is needed to design techniques targeted for deployment on IoT devices.

Artificial intelligence (AI) and Machine learning (ML) on encrypted data: AI has been deployed in almost every aspect of our lives as it can boost significant improvements in systems. ADL are no exception. Many ADL systems use AI/ML models at their core. As pointed out earlier, the data used in these systems are privacy-invasive. Hence, we need to develop practical and reliable AI/ML models that operate on encrypted data. There are already developments in this area; however, these are still far away from being practical for deployment in IoT devices.

Conclusions

We analysed generic ADL systems for detecting abnormal behaviour and highlighted the lack of appropriate protection of users' privacy in such systems. More specifically, we identified three major privacy issues - *identity privacy*, *data confidentiality* and *metadata data leakage* - that are particularly relevant to the ADL systems. To address these issues, we proposed several potential countermeasures. To show the effectiveness of our countermeasures, we took a simple yet effective ADL system and suggested concrete countermeasures to design a system that offers the same (or similar) level of accuracy in ADL analyses but with much higher level of user privacy protection.

We also suggested three future research directions – *practical frictionless authentication*, *efficient secure computation* and *AI/ML on encrypted data* – that needs further exploration before the suggested countermeasure are fully practical and deployable in real-word scenarios.

References

1. M. P. Lawton and E. M. Brody, "Assessment of older people: self-maintaining and instrumental activities of daily living," The gerontologist, vol. 9, no. 3 Part 1, pp. 179–186, 1969.
2. C. Gomez *et al.*, "Internet of things for enabling smart environments: A technology-centric perspective," *J. of Ambient Intelligence and Smart Environments*, vol. 11, no. 1, pp. 23–43, 2019.
3. D. Eckhoff and I. Wagner, "Privacy in the smart city—applications, technologies, challenges, and solutions," *IEEE Communications Surveys Tutorials*, vol. 20, no. 1, pp. 489–516, 2018.
4. N. Suryadevara *et al.*, "Wireless sensors network based safe home to care elderly people: Behaviour detection," *Sensors and Actuators A: Physical*, vol. 186, pp. 277–283, 2012.
5. A. Lotfi *et al.*, "Smart homes for the elderly dementia sufferers: identification and prediction of abnormal behaviour," *J. of Ambient Intelligence and Humanized Computing*, vol. 3, no. 3, pp. 205–218, 2012.
6. O. Aran *et al.*, "Anomaly detection in elderly daily behaviour in ambient sensing environments," in *Human Behavior Understanding*, Springer International Publishing, 2016, pp. 51–67.
7. M. Garcia-Constantino, A. Konios, and C. Nugent, "Modelling activities of daily living with petri nets," in *Int. Conf. on Pervasive Computing and Communications Workshops*, 2018, pp. 866–871.
8. A. Konios *et al.*, "Unifying and analysing activities of daily living in extra care homes," in *Int. Conf. on Dependable, Autonomic and Secure Computing*, on *Pervasive Intelligence and Computing*, on *Big Data Intelligence and Computing and Cyber Science and Technology Congress*, 2018, pp. 474–479.
9. M. Garcia-Constantino *et al.*, "Probabilistic analysis of abnormal behaviour detection in activities of daily living," in *Int. Conf. on Pervasive Computing and Communications Workshops*, 2019, pp. 461–466.
10. A. Konios *et al.*, "Probabilistic analysis of temporal and sequential aspects of activities of daily living for abnormal behaviour detection," in *Int. Conf. on Ubiquitous Intelligence and Comp.*, 2019, pp. 723-730.
11. T. Van hamme *et al.*, "Frictionless authentication systems: Emerging trends, research challenges and opportunities," in *SECURWARE'17*, IARIA, 2017.
12. M. A. Mustafa, A. Abidin, and E. A. Rua, "Frictionless authentication system: Security & privacy analysis and potential solutions," in *SECURWARE'17*, IARIA, 2017.
13. A. Abidin, A. Aly, and M. A. Mustafa, "Collaborative authentication using threshold cryptography," in *ETAA'19*, 2019, pp. 122-137.
14. J. Rafferty *et al.*, "SensorCentral: A Research Oriented, Device Agnostic, Sensor Data Platform," in *Ubiquitous Computing and Ambient Intelligence*, 2017, pp. 97–108.
15. D. Preuveneers and W. Joosen, "Privacy-enabled remote health monitoring applications for resource constrained wearable devices," in *SAC'16*, New York, NY, USA: ACM, 2016, pp. 119–124.

Affiliations

Mustafa A. Mustafa is with The University of Manchester and KU Leuven.
Alexandros Konios is with Staffordshire University.
Matias Garcia-Constantino is with Ulster University.

Biographies

Mustafa A. Mustafa (mustafa.mustafa@manchester.ac.uk) is a Research Fellow at The University of Manchester and KU Leuven. He received a B.Sc degree in Communications from the Technical University of Varna, Bulgaria, in 2007, an M.Sc degree in Communications and Signal Processing from Newcastle University, UK, in 2010, and a Ph.D degree in Computer Science from The University of Manchester, UK, in 2015. His research interests include information security, user privacy and applied cryptography in areas such as smart grid, smart city, e-health, and IoT.

Alexandros Konios (alexandros.konios@staffs.ac.uk) is a Senior Lecturer in Computer Science at Staffordshire University. He obtained his Ph.D degree in Computer Science from Newcastle University, UK. He also holds an M.Sc degree in Computer Security and Resilience from Newcastle University, UK, and a B.Sc degree in Computer Science from the University of Piraeus, Greece. His research interests centre on the analysis of interactive, concurrent and distributed systems, including both the theoretical aspects of their semantics and the application of formal techniques to the modelling and verification of such systems. His interest also involves the development of efficient formal techniques to model and analyse safety-critical systems, such as robotic systems, medical devices and intelligent systems.

Matias Garcia-Constantino (m.garcia-constantino@ulster.ac.uk) is a Lecturer of Computing Science with the School of Computing, Ulster University, UK. He received a bachelor's degree in Computer Engineering from the National Autonomous University of Mexico (UNAM), in 2007, and a Ph.D degree in Computer Science from the University of Liverpool, UK, in 2013. He has experience working in industry and in academia. He worked in Mexico City in two consulting companies as a Java Programmer and as a Data Analyst, respectively. He has worked as a Researcher of Computer Science at the universities of Liverpool, Newcastle, and Ulster. His research interests include data analysis, connected health, pervasive computing, and legal technology.

Acknowledgements

This work was supported in part by Invest Northern Ireland under the Competence Centre Programs Grant RD0513853 - Connected Health Innovation Centre and by the EPSRC through the project EnnCore (EP/T026995/1). The work of Mustafa A. Mustafa is supported by the Dame Kathleen Ollerenshaw Fellowship of The University of Manchester.