Engineering Adaptive Authentication

Alzubair Hassan
Lero@University College Dublin
Ireland
alzubair.mohamedtahir@ucd.ie

Bashar Nuseibeh
The Open University, UK &
Lero@University of Limerick, Ireland
Bashar.Nuseibeh@lero.ie

Liliana Pasquale
Lero@University College Dublin
Ireland
liliana.pasquale@ucd.ie

***Abstract*—Adaptive authentication systems identify and enforce suitable methods to verify that someone (user) or something (device) is eligible to access a service or a resource. An authentication method is usually adapted in response to changes in the security risk or the user's behaviour. Previous work on adaptive authentication systems provides limited guidance about i) what and how contextual factors can affect the selection of an authentication method; ii) which requirements are relevant to an adaptive authentication system and iii) how authentication methods can affect the satisfaction of the relevant requirements. In this paper, we provide a holistic framework informed by previous research to characterize the adaptive authentication problem and support the development of an adaptive authentication system. Our framework explicitly considers the contextual factors that can trigger an adaptation, the requirements that are relevant during decision making and their trade-offs, as well as the authentication methods that can change as a result of an adaptation. From the gaps identified in the literature, we elicit a set of challenges that can be addressed in future research on adaptive authentication.**

***Index Terms*—Adaptive Authentication, Authentication Method, Requirements, Context**

I. Introduction

Authentication verifies that someone (people) or something (device) is eligible to access specific services or resources [1]. This process typically requires users to provide identification credentials, such as a combination of a username and a password, to an authentication system. Many organizations, such as Amazon and Google, increasingly require their users to provide at least two types of credentials during authentication (two-factor authentication) to strengthen the defence against users' account compromise. However, choosing the same type of authentication may not always be effective in application domains, such as smart cities and transport, where contextual factors and requirements priorities can change [2]. For example, password-based authentication may not be suitable when a user is driving a car, since in this context, automation requirements can have a higher priority over other requirements, such as confidentiality.

Adaptive security systems [3], [4] mitigate varying security threats and continuously protect valuable assets by changing security controls at runtime. An adaptive authentication system (e.g., [5]–[8]) is an adaptive security system that attempts to match the required authentication credentials to the perceived risk of the authorization requested. The objective is to reduce the authentication burden on users, while enforcing strong authentication where it is most needed. For example, passengers of a public transport system who access live information about bus timetables should not use a strong authentication, since the risk of information exfiltration is low. However, accessing sensitive information, such as a work email, using public WiFi should require stronger authentication (e.g., two-factor authentication), as the risk of information exfiltration is high.

In this paper argue that building adaptive authentication systems poses additional challenges to adaptive security. A multitude of contextual factors (e.g., assets sensitivity, execution platform, user experience) can affect security risks and requirements priorities in ways that cannot always be foreseen at design time. It is also difficult to select an effective authentication method, as its impact on the satisfaction of requirements may be hard to quantify. Previous work on adaptive authentication [1], [9] provides limited guidance on how adaptive authentication systems can be built systematically. Thus, a number of open issues still remain: i) which requirements are relevant to an adaptive authentication system, ii) how contextual factors can affect the feasibility of authentication methods, and iii) how different authentication methods can affect satisfaction of the requirements. Although previous work on adaptive systems has considered context-driven adaptation (e.g., [10]–[12]), it has not taken into account how context can affect the priority of the requirements and the feasibility of authentication methods. Also, authentication is highly personal, and users' preferences and privacy requirements can affect adaptation decisions.

In this paper we propose a framework, informed by previous research, to characterize the adaptive authentication problem and to support engineering of adaptive authentication systems. Our framework elicits: a) the requirements that are relevant during decision making and their trade-offs; b) the contextual factors that can trigger an adaptation and how they can affect the security risks and requirements priorities; and c) the authentication methods that can change as a result of an adaptation and their effectiveness. To motivate the adaptive authentication problem we discuss a set of scenarios in the Internet of Vehicles (IoV) domain. From the gaps identified in the literature, we elicit a set of challenges for future research on adaptive authentication.

II. Authentication Scenarios in IoV

The scenarios presented in this section are informed by potential attacks in different IoV network topologies and applications/services [13]. The IoV network [14] is a heterogeneous

vehicular network combining inter-vehicle and intra-vehicle networks, and vehicular mobile Internet.

The ambulance needs to acquire road traffic information to reach the hospital as soon as possible. To achieve this aim, it communicates with the nearest roadside units (RSU) using a Vehicle-to-Roadside units (V2R) topology (see Figure 1a). The nearby cars can potentially impersonate the ambulance acquiring road traffic information illegitimately. In this scenario, the requirements related to the confidentiality of the road traffic information and authenticity of the parties sharing information (ambulance and RSU) have higher priority compared to usability and performance requirements. To decrease the risk of impersonation attack, the ambulance and the RSU should use, for example, a certificate-based authentication or signcryption-based authentication, before they start sharing information.

The ambulance is trying to overtake the red car (see Figure 1b). To achieve this aim, the ambulance needs to exchange with the nearby cars (red and the blue car) information about their respective distance using a Vehicle-to-Vehicle (V2V) communication topology. Maintaining integrity of distance information is highly important to avoid vehicle crashes. The exchange of distance information should happen quickly to allow the ambulance to overtake the red car in a timely manner. Thus, performance requirements (e.g., minimize the time to perform authentication) should have a higher priority compared to security and usability requirements. Using a certificate-based authentication is not appropriate in this situation, since it can require excessive time to verify the identity of the vehicles on a remote server. Alternatively, the vehicles can use the car plate and the driver license to authenticate with one another. These credentials can be transmitted and verified in a shorter time compared to certificate-based authentication, and can avoid impersonation attacks.

The ambulance driver is at a junction and is accessing information about the patient using a Vehicle-to-Infrastructure of cellular networks (V2I) (see Figure 1c). Because the accessed information is sensitive, maintaining its confidentiality is highly important. Usability requirements are also important, since the authentication method should not distract the driver, while s/he needs to focus on crossing the junction. For example, a biometrics-based authentication (e.g., face or iris recognition) can be ideal in this scenario because it does not require an input from the driver.

Many contextual factors (e.g., location, network topology, sensitivity of accessed information, proximity with other vehicles) can affect the security risk and the priority of the requirements that can be relevant during adaptive authentication (e.g., security, usability and performance). These requirements can also be conflicting with one another. For example, adopting a strong authentication technique can harm performance (e.g., a certificate-based authentication) and also usability requirements (e.g., a password that is very hard to remember). Certain contextual factors (e.g., low lighting) can render some authentication methods (e.g., face recognition) ineffective. Moreover, estimating the impact that an authentication method has on the requirements cannot be quantified precisely. Finally, since users can actively engage in the authentication, their preferences and privacy requirements should be taken into account when an authentication method is selected.

III. Adaptive Authentication

An adaptive authentication system monitors contextual factors and behavioural features of its users to identify changing security risks. The system can decide to enforce an authentication method to mitigate the security risks and maximise user convenience [1], [9], [15]. For example, Hayashi et al. [8] associate a risk level with the location from where a user requests access (home, work, other). If the user tries to access a service/resource from a previously unknown location, s/he is required to provide additional credentials (e.g., pin, password). Security risks can also be brought by changes in user habits. For example, Gebrie and Abie [5] consider the change in users' daily routines (e.g. walking, eating, sleeping) monitored using wearable devices, to calculate the risk score of an access request. They link the risk score to an abnormal activity and adapt the authentication method accordingly.

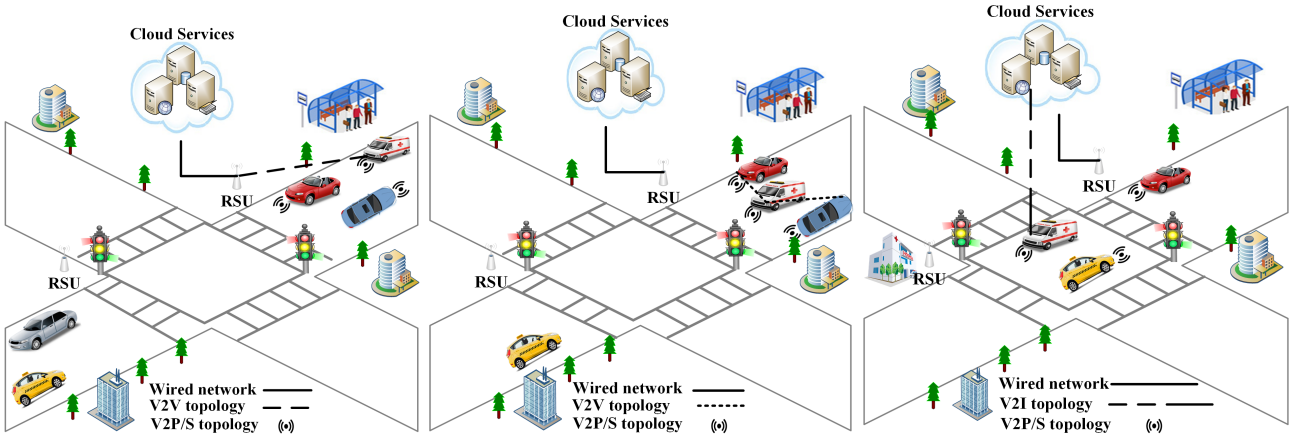
Continuous authentication [16], instead, refers to the activities performed after a user has authenticated successfully, to ensure that the session continues to be held by the legitimate user. It also aims to ensure that the user experience is maximized, for example, by reducing the frequency with which a user is required to re-authenticate. A continuous authentication system usually monitors the user behaviour (e.g., applications usage, pressure on touch screens) to identify security risks arising after a user authenticates successfully. For example, Karanikiotis et al. [17] monitor the users'gestures (e.g., swipes) on a mobile device. If the user exhibits abnormal gestures, s/he is classified as an illegitimate user and the mobile device is locked automatically. However, this approach is not suitable when a legitimate user is simply performing a new behaviour. In such a situation, continuous authentication should be combined with adaptive authentication. For example, Jorquera et al. [18] uses machine learning to identify whether the owner of a mobile device is legitimate depending on his/her application usage statistics. The system considers the usage statistics falling in the possibly normal category to learn new behaviours, and triggers re-authentication if the AL score falls in one of the anomalous categories.

IV. Adaptive Authentication Framework

We reviewed previous work on adaptive authentication and leveraged our authentication scenarios to elicit the main aspects to be considered when building an adaptive authentication system: requirements, authentication methods, contextual factors, and decision-making techniques.

A. Requirements

The requirements of an adaptive authentication system are mainly related to security, privacy, usability, and performance. The majority of the adaptive authentication systems (e.g., [5]–[8], [15], [18]–[22]) that we examined adapt the authentication method as a result of a changing security risk. For example, De



(a) (b) (c)

Fig. 1: IoV Adaptive Authentication Scenarios.

Silva et al. [15] link specific changes in the user profile (e.g., location, browser type, mouse behaviour, keystroke patterns) to changes in the security risk. When a high-security risk is detected, a stronger authentication method (e.g., two-factor authentication) is enforced. Daud et al. [20] link the user's login attempts to the security risk based on contextual factors, such as the IP address, location, type of browser, and the operating system. In case of an increased risk, this approach applies penalties, for example, it can adopt 2- or 3-factor authentication, it can block authentication for a given period of time, or blacklist a user. Although it has not been considered in previous work on adaptive authentication, an important requirement is authenticity. This requirement is relevant in the scenario shown in Figure 1a, where the selection of a certificate-based authentication is dictated by the need to ensure authenticity of the communicating parties.

Some approaches surveyed, especially those based on user behaviour and using physiological credentials, aim to satisfy *privacy* requirements, particularly anonymity and untraceability [13], [23]–[25]. For example, Xi et al. [25] propose an adaptive anonymous authentication protocol in a V2R topology based on a cryptographic technique called verifiable common secret encoding. This technique uses the cryptographic keys of the communicating users to hide their individual identities. The authentication protocol can also adapt at runtime depending on the level of anonymity required by the users.

Because authentication can be performed by humans, it is also crucial to consider *usability* requirements. These mainly aim to maximize the quality of the user experience during authentication. Usability has been mainly considered in terms of ease of use, for users having different behaviors [18], abilities [26], and ages [27]. Other work [28] has considered usability in terms of transparency, i.e. the system should provide users with explanations justifying why it changed the required authentication method. Usability is also commonly expressed in terms of efficiency and effectiveness of the authentication methods [29]. More precisely, *efficiency* is related to the speed of the authentication method. For example, Jorquera et al. [18] minimize the number of authentication credentials to improve efficiency. Effectiveness is related to the error rate that an authentication method can be prone to. This can be related to the memorability of the credentials (e.g., using a password that is difficult to remember can be ineffective) and also to environmental factors (e.g., noise type and level, lighting level, or temperature) [30]. Other work [21], instead, aims to maximize satisfaction of the *user's preferences*, by allowing a user to select an authentication method for specific applications. This can be relevant when users prefer stronger authentication techniques in specific contexts: work, personal account, and financial [31].

Although performance requirements have been briefly mentioned in previous work [21], [32]–[34], their distinction with usability requirements has not been defined clearly. From our analysis, *performance* requirements can be about minimize the authentication time. Authentication time is related to the time necessary to provide the required credentials to the system, while authentication delay is related to the time necessary to validate the credentials. Finally, only a few approaches [18], [21] address the trade-off between the aforementioned requirements, mainly focusing on security and usability requirements.

B. Authentication Methods

The authentication methods that have been used in previous work have optional and mandatory authentication features. It is mandatory to choose a credential type [35], such as something you know (e.g., password, OTP), something you have (e.g., smartcard, token), something you are (e.g., face, iris, fingerprint), or two-factor authentication (e.g., select two credentials). The credential type affects the level of automation. For example, iris and face recognition have the highest level of automation, since they require the minimum input from the user. Fingerprint-based authentication has a medium level of automation since it requires the user to actively scan his/her finger. Password-based authentication has a low level

of automation since it requires the user to remember and input a password. Some authentication features, such as credentials renewal [28], [33] and cryptography type [25], [35], are optional. Others require specific devices to be performed [21], [31] (e.g., smartcard-based authentication requires a reader). Representing the features of an authentication method can help express its impact on the satisfaction of the requirements.

C. Contextual Factors

We group contextual factors depending on whether they affect 1) the security risk and the adaptive authentication requirements or 2) the feasibility of authentication methods.

1) Security risks and requirements:

- *Assets Sensitivity* refers to the criticality of data or applications to which access is requested. Asset sensitivity can increase the priority of security requirements and also affect security risks. Thus, some approaches (e.g., [21], [36]) adapt the authentication method depending on the sensitivity of the data to be accessed.
- *Location* refers to the place where a user is authenticating and can have an impact on the security risks. Several approaches have proposed to ask the user for additional credentials, if s/he attempts to access services/resources from an unusual location [7], [19], [20], [37].
- *Network Topology* can affect the security risk. Previous work [13] suggests to change authentication method depending on the attacks that can exploit the topology of the network a node is currently connected to.
- *Time* refers to the moment when authentication is performed and can also affect security risks [7], [19], [20]. For example, if a user tries to access an asset in odd times (e.g., outside the working hours) s/he can be asked to provide additional credentials during authentication [7], [19] or can be subjected to penalties (e.g., being blocked for some hours or permanently) [20].
- *User Role* (e.g., manager VS regular employee [38]) can affect the security risk. Arfaoui et al. [22] require the nodes of an Internet of Things (IoT) network to adopt an authentication method depending on their role (e.g., IoT gateway, context manager, data consumer) and also depending on additional contextual information (e.g., location, time, emergency situation, normal situation). In the scenario shown in Figure 1a, the role of an actor (e.g., ambulance) can also increase the priority of the authenticity requirement.
- *Movement of the Nodes* refers to the movement of the nodes within a network. For example, in an IoV network nodes can change their position, requiring authentication to be performed rapidly. As shown in the scenario in Figure 1b, the presence of moving authenticating vehicles increases the priority of performance requirements. Fayad et al. [32] proposed an adaptive authentication approach where nodes of an IoT network can store their authentication information on the blockchain. This allows authentication to be performed even when the authenticating nodes do not belong to the same network.
- *User Preferences* refer to users favoring specific authentication methods to others [7], [20], [21], [30], [39]. Considering user preferences during adaptive authentication can increase satisfaction of usability requirements.

2) Feasibility of authentication methods:

- *Authentication Devices* refer to the devices (e.g, phone, camera, reader) available to perform authentication. For example, some authentication methods (e.g., RFID) require additional devices (e.g., reader) [40]. In other situations, limited-resources devices may not be able to support authentication methods that are computationally intensive (e.g., cryptography-based authentication) [18].
- *Proximity* refers to the user's distance from a device and can indicate possession of the device [41]. For example, two-factor authentication can be enabled by sending a PIN to the device a user is close to.
- *Device Position* refers to the relative position of a device w.r.t. its owner (e.g., held on hand or in the pocket). For example, face recognition is not feasible if the device is held in the pocket. Frequent changes of the device position can make gait-based authentication infeasible [42].
- *Network Quality* can affect feasibility of authentication methods (e.g. cryptography-based authentication) that can have overheads in the communication network. For example, in IoV the use of a network with limited bandwidth can cause delays and even lead to fatal accidents [13].
- *Environmental Conditions* refer to conditions, such as lighting and noise level. For example, Wojtowicz and Joachimiak [30] propose a system that avoids selecting authentication methods that may not be effective in certain environmental conditions. For example, face recognition and voice recognition are avoided when the lighting level is low and the noise level is high, respectively.

Although in this paper we have identified relationships between contextual factors and requirements, existing adaptive authentication approaches have only focused on specific contextual factors relevant to the considered application domain.

D. Decision-Making Techniques

Various decision-making methods have been used in previous work on adaptive authentication. For example, machine learning has been used to learn the features characterizing the user's behaviour and the power consumption of the devices [5], [8], [15], [18], [21], [42], [43]. Rule-based reasoning has been used to adjust the authentication method based on the security risk [7], [20], [30], [34], [36], [44], [45]. Optimization methods have been used to select an optimal authentication method depending on environmental conditions [30], [33]. However, these techniques have only considered the impact of a small set of contextual factors on the feasibility of the authentication methods. Also, they have not considered how different authentication methods can affect requirements that are different than security.

V. Adaptive Authentication Challenges

Authentication is highly personal, and users' preferences and privacy requirements can affect adaptation decisions.Therefore, we elicit a set of challenges that can be addressed in future research on adaptive authentication.

i) Represent requirements, contextual factors and authentication methods. The goal models [46] can be adopted to represent the impact of the contextual factors that were relevant in our IoV scenarios on the security risk and the feasibility of the authentication techniques. Also, the feature models [47] can be adopted to represent the impact of an authentication methods on the satisfaction of the requirements. However, identifying a qualitative weight to express the impact of these relationships was challenging because these have not been discussed thoroughly in previous work. The catalog of requirements and contextual factors provided in this paper can be beneficial for this purpose. Also it will be necessary to identify ways to use the information coming from the goal model and the feature model to compute utility of authentication methods and select an optimal one. Fuzzy Causal Networks [3] and theorem provers [48] can be adopted for this purpose, but they will require to update the model used for reasoning at runtime.

ii) Monitor changes in contextual factors. Several contextual factors can impact the priority of the requirements and the feasibility of authentication methods. Also , a different set of contextual factors can become more relevant in different situations. For example, the movement of nodes is more relevant when the ambulance is trying to overtake the red car (Figure 1b) and the lighting level becomes more relevant when the ambulance driver is at a junction (Figure 1c). Due to the multitude of contextual factors, it is not possible to monitor their changes continuously. Thus, there is a need for monitoring approaches able to collect data to detect specific situations (e.g., a vehicle trying to overtake another one, crossing a junction) and identify suitable monitor activities to be performed in those situations.

iii) Tune decision-making depending on the time available. In some cases, the decision-making in an adaptive system can depend on the time available. For example, in emergency situations (e.g., an ambulance needs to reach the hospital quickly with the patient) the authentication with RSU and vehicle on the road needs to be performed very fast. Accordingly, the decision of choosing an effective authentication method should be performed quickly. A possible way to support this activity is to identify strategies to selectively remove less relevant elements from the models used to support decision making. For example, a smaller set of authentication methods and contextual factors can be considered to compute the security risk and support decision making.

iv) Tame Uncertainty. From our initial study we noticed that there is uncertainty concerning the impact of authentication methods and user's preferences on the satisfaction of the requirements (e.g., security, usability, performance). Although the impact of an authentication method on the performance requirements can be assessed precisely, the same does not apply to other requirements, such as security and usability. Thus, it will be necessary to identify appropriate techniques to update the impact that authentication methods can have on the satisfaction of security requirements, for example, considering information available in existing vulnerability repositories.

v) Combine Adaptive and Continuous Authentication. In certain cases, authentication needs to be re-performed over time, for example, to ensure that the ambulance still corresponds to a legitimate user. To decide when authentication should be re-performed, it will be necessary to collect information about the user behaviour and contextual factors to identify anomalies which should force re-authentication. Similarly as for adaptive authentication, the authentication method enforced will depend on the requirements, contextual factors and the security risks.

VI. Conclusion and Future work

In this paper, we proposed a framework, informed by previous research, to characterize the adaptive authentication problem and support the engineering of adaptive authentication systems. We elicited a set of challenges for the community to address in future research on adaptive authentication. We suggested that these challenges could be generalised to other user-facing security controls.

For future work, we plan to improve our initial taxonomy to eliciting requirements, contextual factors and authentication methods to support engineering adaptive authentication. We will investigate the use of live models to represent and update these concepts and their mutual impact at runtime. Finally, we will explore novel monitoring approaches to identify changing situations and select, for each situation, the contextual factors to be monitored and the time available to support decision making. This will allow us to adjust the size of the model used to support decision-making depending on the situation.

Acknowledgment

This publication was supported by the EU H2020 CyberSec4Europe project (grant number 830929) and by Science Foundation Ireland under Grant number 13/RC/2094_P2.

References

[1] K. A. A. Bakar and G. R. Haron, "Adaptive authentication: Issues and challenges," in *2013 World Congress on Computer and Information Technology*. IEEE, 2013, pp. 1–6.

[2] C. Katsini, M. Belk, C. Fidas, N. Avouris, and G. Samaras, "Security and usability in knowledge-based user authentication: A review," in *Proc. of the 20th Pan-Hellenic Conf on Informatics*, 2016, pp. 1–6.

[3] M. Salehie, L. Pasquale, I. Omoronyia, R. Ali, and B. Nuseibeh, "Requirements-Driven Adaptive Security: Protecting Variable Assets at Runtime," in *Proc. of the 20th IEEE Int. Requirements Engineering Conf.*, 2012, pp. 111–120.

[4] E. Yuan, N. Esfahani, and S. Malek, "A systematic survey of self-protecting software systems," *ACM Trans. Auton. Adapt. Syst.*, vol. 8, no. 4, pp. 17:1–17:41, 2014.

[5] M. T. Gebrie and H. Abie, "Risk-based adaptive authentication for internet of things in smart home ehealth," in *Proc. of the 11th European Conf on Software Architecture: Companion Proc.*, 2017, pp. 102–108.

[6] S. Gupta, A. Buriro, and B. Crispo, "Driverauth: A risk-based multi-modal biometric-based driver authentication scheme for ride-sharing platforms," *Computers & Security*, vol. 83, pp. 122–139, 2019.

[7] K. A. A. Bakar and G. R. Haron, "Adaptive authentication based on analysis of user behavior," in *2014 Science and Information Conf.* IEEE, 2014, pp. 601–606.

[8] E. Hayashi, S. Das, S. Amini, J. Hong, and I. Oakley, "Casa: context-aware scalable authentication," in *Proc. of the Ninth Symposium on Usable Privacy and Security*, 2013, pp. 1–10.

[9] P. Arias-Cabarcos, C. Krupitzer, and C. Becker, "A survey on adaptive authentication," *ACM Computing Surveys*, vol. 52, no. 4, pp. 1–30, 2019.

[10] A. Bucchiarone, R. Kazhamiakin, C. Cappiello, E. Di Nitto, and V. Mazza, "A context-driven adaptation process for service-based applications," in *Proc. of the 2nd Int Workshop on Principles of Engineering Service-Oriented Systems*, 2010, pp. 50–56.

[11] G. Tamura, N. M. Villegas, H. A. Muller, L. Duchien, and L. Seinturier, "Improving context-awareness in self-adaptation using the dynamico reference model," in *2013 8th Int Symposium on Software Engineering for Adaptive and Self-Managing Systems*. IEEE, 2013, pp. 153–162.

[12] L. Kulp, A. Sarcevic, M. Cheng, and R. S. Burd, "Towards dynamic checklists: Understanding contexts of use and deriving requirements for context-driven adaptation," *ACM Transactions on Computer-Human Interaction*, vol. 28, no. 2, pp. 1–33, 2021.

[13] S. Sharma and B. Kaushik, "A survey on internet of vehicles: Applications, security issues & solutions," *Vehicular Communications*, vol. 20, p. 100182, 2019.

[14] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C.-T. Lin, and X. Liu, "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.

[15] H. De Silva, D. C. Wittebron, A. R. Lahiru, K. L. Madumadhavi, L. Rupasinghe, and K. Y. Abeywardena, "Authdna: An adaptive authentication service for any identity server," in *2019 Int. Conf. on Advancements in Computing*. IEEE, 2019, pp. 369–375.

[16] S. Eberz, K. B. Rasmussen, V. Lenders, and I. Martinovic, "Evaluating behavioral biometrics for continuous authentication: Challenges and metrics," in *Proc. of the 2017 ACM on Asia Conf on Computer and Communications Security*, 2017, pp. 386–399.

[17] T. Karanikiotis, M. D. Papamichail, K. C. Chatzidimitriou, N.-C. I. Oikonomou, A. L. Symeonidis, and S. K. Saripalle, "Continuous implicit authentication through touch traces modelling," in *2020 IEEE 20th Int. Conf. on Software Quality, Reliability and Security*. IEEE, 2020, pp. 111–120.

[18] J. M. Jorquera Valero, P. M. Sánchez Sánchez, L. Fernández Maimó, A. Huertas Celdrán, M. Arjona Fernández, S. De Los Santos Vílchez, and G. Martínez Pérez, "Improving the security and qoe in mobile devices through an intelligent and adaptive continuous authentication system," *Sensors*, vol. 18, no. 11, p. 3769, 2018.

[19] N. I. Daud, G. R. Haron, and S. S. S. Othman, "Adaptive authentication: Implementing random canvas fingerprinting as user attributes factor," in *2017 IEEE Symposium on Computer Applications & Industrial Electronics*. IEEE, 2017, pp. 152–156.

[20] N. I. Daud, G. R. Haron, and D. Din, "Adaptive authentication to determine login attempt penalty from multiple input sources," in *2019 IEEE Conf on Application, Information and Network Security*. IEEE, 2019, pp. 1–5.

[21] O. Riva, C. Qin, K. Strauss, and D. Lymberopoulos, "Progressive authentication: deciding when to authenticate on mobile phones," in *Presented as part of the 21st USENIX Security Symposium*, 2012, pp. 301–316.

[22] A. Arfaoui, S. Cherkaoui, A. Kribeche, S. M. Senouci, and M. Hamdi, "Context-aware adaptive authentication and authorization in internet of things," in *IEEE Int. Conf. on Communications*. IEEE, 2019, pp. 1–6.

[23] A. Hassan, A. A. Omala, M. Ali, C. Jin, and F. Li, "Identity-based user authenticated key agreement protocol for multi-server environment with anonymity," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 890–902, 2019.

[24] K. Sha, Y. Xi, W. Shi, L. Schwiebert, and T. Zhang, "Adaptive privacy-preserving authentication in vehicular networks," in *2006 First Int. Conf. on Communications and Networking in China*. IEEE, 2006, pp. 1–8.

[25] Y. Xi, K.-W. Sha, W.-S. Shi, L. Schwiebert, and T. Zhang, "Probabilistic adaptive anonymous authentication in vehicular networks," *Journal of Computer Science and Technology*, vol. 23, no. 6, pp. 916–928, 2008.

[26] R. Kainda, I. Flechais, and A. Roscoe, "Security and usability: Analysis and evaluation," in *2010 Int. Conf. on Availability, Reliability and Security*. IEEE, 2010, pp. 275–282.

[27] J. Nicholson, L. Coventry, and P. Briggs, "Age-related performance issues for pin and face-based authentication systems," in *Proc. of the SIGCHI Conf on Human Factors in Computing Systems*, 2013, pp. 323–332.

[28] S. Ruoti, B. Roberts, and K. Seamons, "Authentication melee: A usability analysis of seven web authentication systems," in *Proc. of the 24th Int. Conf. on World Wide Web*, 2015, pp. 916–926.

[29] E. Frøkjær, M. Hertzum, and K. Hornbæk, "Measuring usability: are effectiveness, efficiency, and satisfaction really correlated?" in *Proc. of the SIGCHI Conf on Human Factors in Computing Systems*, 2000, pp. 345–352.

[30] A. Wójtowicz and K. Joachimiak, "Model for aptable context-based biometric authentication for mobile devices," *Personal and Ubiquitous Computing*, vol. 20, no. 2, pp. 195–207, 2016.

[31] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons, "A usability study of five two-factor authentication methods," in *Fifteenth Symposium on Usable Privacy and Security*, 2019.

[32] A. Fayad, B. Hammi, and R. Khatoun, "An adaptive authentication and authorization scheme for iot's gateways: a blockchain based approach," in *2018 Third Int. Conf. on Security of Smart Cities, Industrial Control System and Communications*. IEEE, 2018, pp. 1–7.

[33] D. Dasgupta, A. Roy, and A. Nag, "Toward the design of adaptive selection strategies for multi-factor authentication," *computers & security*, vol. 63, pp. 85–116, 2016.

[34] I. You, J. D. Lim, J. N. Kim, H. Ahn, and C. Choi, "Adaptive authentication scheme for mobile devices in proxy mipv6 networks," *IET Communications*, vol. 10, no. 17, pp. 2319–2327, 2016.

[35] A. Hassan, N. Eltayieb, R. Elhabob, and F. Li, "An efficient certificateless user authentication and key exchange protocol for client-server environment," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 6, pp. 1713–1727, 2018.

[36] J. Seifert, A. De Luca, B. Conradi, and H. Hussmann, "Treasurephone: Context-sensitive user data protection on mobile phones," in *Int. Conf. on Pervasive Computing*. Springer, 2010, pp. 130–137.

[37] R. Hulsebosch, M. S. Bargh, G. Lenzini, P. Ebben, and S. M. Iacob, "Context sensitive adaptive authentication," in *European Conf on Smart Sensing and Context*. Springer, 2007, pp. 93–109.

[38] D. Goel, E. Kher, S. Joag, V. Mujumdar, M. Griss, and A. K. Dey, "Context-aware authentication framework," in *Int. Conf. on Mobile Computing, Applications, and Services*. Springer, 2009, pp. 26–41.

[39] A. Forget, S. Chiasson, P. C. Van Oorschot, and R. Biddle, "Improving text passwords through persuasion," in *Proc. of the 4th symposium on Usable privacy and security*, 2008, pp. 1–12.

[40] B. Mbarek, M. Ge, and T. Pitner, "Self-adaptive rfid authentication for internet of things," in *Int. Conf. on Advanced Information Networking and Applications*. Springer, 2019, pp. 1094–1105.

[41] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca, "Ensemble: cooperative proximity-based authentication," in *Proc. of the 8th Int. Conf. on Mobile systems, applications, and services*, 2010, pp. 331–344.

[42] A. Primo, V. V. Phoha, R. Kumar, and A. Serwadda, "Context-aware active authentication using smartphone accelerometer measurements," in *Proc. of the IEEE Conf on computer vision and pattern recognition workshops*, 2014, pp. 98–105.

[43] Z. Cui, Y. Zhao, C. Li, Q. Zuo, and H. Zhang, "An adaptive authentication based on reinforcement learning," in *2019 IEEE Int. Conf. on Consumer Electronics-Taiwan*. IEEE, 2019, pp. 1–2.

[44] W. Xu, Y. Shen, Y. Zhang, N. Bergmann, and W. Hu, "Gait-watch: A context-aware authentication system for smart watch based on gait recognition," in *Proc. of the Second Int. Conf. on Internet-of-Things Design and Implementation*, 2017, pp. 59–70.

[45] A. Mansour, M. Sadik, E. Sabir, and M. Azmi, "A context-aware multimodal biometric authentication for cloud-empowered systems," in *2016 Int. Conf. on Wireless Networks and Mobile Communications*. IEEE, 2016, pp. 278–285.

[46] A. Van Lamsweerde, *Requirements engineering: From system goals to UML models to software*. Chichester, UK: John Wiley & Sons, 2009, vol. 10.

[47] K. C. Kang, S. G. Cohen, J. A. Hess, W. E. Novak, and A. S. Peterson, "Feature-oriented domain analysis (foda) feasibility study," Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst, Tech. Rep., 1990.

[48] L. Pasquale, P. Spoletini, M. Salehie, L. Cavallaro, and B. Nuseibeh, "Automating trade-off analysis of security requirements," *Requirements Engineering*, vol. 21, no. 4, pp. 481–504, 2016.