

Risk-Based Adaptive User Authentication for Mobile Passenger ID Devices for Land/Sea Border Control

Maria Papaioannou
Instituto de Telecomunicações
Aveiro, Portugal
Faculty of Engineering and Science,
University of Greenwich
Chatham Maritime, UK
m.papaioannou@av.it.pt

Georgios Mantas
Instituto de Telecomunicações
Aveiro, Portugal
Faculty of Engineering and Science,
University of Greenwich
Chatham Maritime, UK
gimantas@av.it.pt

Aliyah Essop
Faculty of Engineering and Science,
University of Greenwich
Chatham Maritime, UK
a.b.essop@greenwich.ac.uk

Phil Cox
Faculty of Engineering and Science,
University of Greenwich
Chatham Maritime, UK
p.w.cox@gre.ac.uk

Ifiok E. Otung
Faculty of Computing, Engineering and
Science, University of South Wales
Pontypridd, UK
ifiok.otung@southwales.ac.uk

Jonathan Rodriguez
Instituto de Telecomunicações
Aveiro, Portugal
Faculty of Computing, Engineering and
Science, University of South Wales
Pontypridd, UK
jonathan@av.it.pt

Abstract—New services and products are increasingly becoming integral parts of our daily lives rising our technological dependence, as well as our exposure to risks from cyber. Critical sectors such as transport are progressively depending on digital technologies to run their core operations and develop novel solutions to exploit the economic strengths of the European Union. However, despite the fact that the continuously increasing number of visitors, entering the European Union through land-border crossing points or seaports, brings tremendous economic benefits, novel border control solutions, such as mobile devices for passenger identification for land and sea border control, are essential to accurately identify passengers “on the fly” while ensuring their comfort. However, the highly confidential personal data managed by these devices makes them an attractive target for cyberattacks. Therefore, novel secure and usable user authentication mechanisms are required to increase the level of security of this kind of devices without interrupting border control activities. Towards this direction, we, firstly, discuss risk-based and adaptive authentication for mobile devices as a suitable approach to deal with the security vs. usability challenge. Besides that, a novel risk-based adaptive user authentication mechanism is proposed for mobile passenger identification devices used by border control officers at land and sea borders.

Keywords—*risk-based user authentication, adaptive user authentication, mobile passenger ID devices, border control security*

I. INTRODUCTION

As innovative services and products take off, they become integral parts of our daily lives in a wide spectrum of applications. Nevertheless, with every new development towards the connectivity of people, processes and things, our dependence to technology rises, and so too does our exposure to risks from cyber, highlighting the importance of cybersecurity for the modern organizations [1], [2]. In particular, the explosive growth of interconnected devices in

combination with the increasing use of artificial intelligence in organizational processes expands the organizations’ open surface to cyberattacks [1], [2]. In addition, the more personal data are available online, the more likely individuals are to fall victim to a form of cyberattack or cybercrime. Consequently, while digitalization brings enormous opportunities and economic benefits providing solutions for the challenges Europe is currently facing, it also exposes the society and economy to cyber threats. Critical sectors such as transport become increasingly dependent on digital technologies to perform their core operations and develop novel efficient transport services and infrastructure to exploit the economic strengths of the EU, and to empower cohesion both at economic and social level [3], [4]. For instance, although the continuously increasing number of visitors entering the European Union through land-border crossing points or seaports brings tremendous economic benefits, novel border control solutions, such as mobile devices for passenger identification for land and sea border control, are essential to accurately identify passengers “on the fly” while ensuring their comfort [4].

Nevertheless, these devices are expected to become an appealing target for malicious actors in terms of data misuse, data loss and data theft as it is anticipated that they will handle highly sensitive and confidential personal data [4], [5]. Consequently, strong user authentication mechanisms are required to ensure high level of device security to protect sensitive data handled by this kind of devices [6], [7], [8], [9], [10]. Since this kind of mobile devices falls into the category of public safety, we began our work with qualitative research, which focuses on the information provided by NIST about public safety mobile authentication. NIST Special Publication 8080 [11] stated that most of the current authentication methods are practically not convenient for the first responders such as the land and sea border control officers, and thus they become infeasible for public safety use in the field. Therefore, it is of utmost importance research effort to be put in the design and implementation of novel secure and usable user authentication mechanisms that will increase the level of device security of the passenger



















The research work leading to this publication has received funding from the European Union’s Horizon 2020 Research and Innovation programme under grant agreement H2020-MSCA-RISE-2019-eBORDER-872878.

identification mobile devices and will ensure that border control officers at land and sea borders are able to successfully complete their missions [4].

However, security and usability are often thought of as being contradictive [4]. To deal with this security vs. usability challenge, risk-based and adaptive user authentication types have been proposed to dynamically authenticate a legitimate user throughout their entire interaction with the mobile device, based on a risk score computed in real-time, and adapt the user authentication method based on this risk score, enhancing the reliability of the whole authentication process without interrupting the user's normal activity [12]. Towards this direction, we, firstly, discuss background concepts on risk-based and adaptive authentication, and a review of related work on user authentication solutions for mobile devices is given. Our target is to provide a foundation for organizing research efforts towards the design and development of effective and efficient risk-based adaptive user authentication mechanisms for mobile passenger identification devices used by border control officers at land and sea borders. Besides that, a novel risk-based adaptive user authentication mechanism is proposed.

Following the Introduction, the rest of the paper is organized as follows. Section II presents a review of related work on user authentication solutions for mobile devices, as well as adaptive and risk-based user authentication. In Section III, a proposed risk-based adaptive user authentication mechanism is provided. Finally, the paper is concluded in Section IV.

TABLE I. USABILITY ANALYSIS SUMMARY OF PUBLIC SAFETY MOBILE AUTHENTICATION METHODS

<i>Authentication Method</i>	<i>Feasible</i>	<i>Challenging</i>	<i>Impractical</i>
No authentication			
Knowledge-based authentication			
Password			
PIN			
Gesture			
OTP device			
Embedded cryptographic token			
Removable hardware cryptographic token			
Smartcard with external reader			
NFC-enabled smartcard			
Proximity token			
Fingerprints			
Facial recognition			
Iris recognition			
Speaker recognition			
Keystroke dynamics			
On-body detection			
Location-based awareness			

II. RELATED WORK

Security and usability are often thought of as being contradictive. In this section, we explore the possibility of incorporating both security and usability in user authentication for mobile passenger identification devices for land and sea border control. In order to meet the objectives for secure and usable user authentication for land and sea border passenger identification mobile devices, it is of utmost importance to conduct research to understand the land and sea border control officers' needs, key characteristics, tasks, and environments [4], [11]. Due to the fact that this kind of mobile devices falls into the category of public safety [4], [11], we began our work with qualitative research, which focuses on the information provided by NIST about public safety mobile authentication. According to NIST Special Publication 8080 [11], most of the current authentication methods are not feasible for public safety use in the field as they are practically not convenient for the first responders (e.g., the land and sea border control officers). In Table I, conventional authentication methods are rated as feasible, challenging, or impractical from a usability perspective based on NIST Special Publication 8080 [11], highlighting the need for novel more sophisticated user authentication mechanisms for public safety applications.

According to NIST Special Publication 8080 [11], the aim is that authentication should not interrupt actively responding first responders, nor should it overburden them in any stage of response. For instance, if authentication can be implemented such that first responders authenticate at the beginning of a shift, and stay authenticated throughout the shift, then many of the existing and commonly implemented authentication methods (e.g., knowledge-based authentication schemes or biometrics) would then become more feasible. To support such a scenario, more sophisticated mechanisms must be implemented to enhance the reliability of whole authentication process without interrupting the land and sea border control officer's normal activity on the field. To deal with this security vs. usability challenge, adaptive and risk-based authentication mechanisms have been proposed to constantly authenticate a legitimate user throughout the entire session [12], [13]. In the rest of this section, we are going to further elaborate the aforementioned types of user authentication.

A. Adaptive Authentication

Adaptive authentication is a way that two-factor authentication or multifactor authentication can be efficiently configured and deployed. In particular, it is a method for selecting the proper authentication factors based on: a.) user's risk profile, and b.) user's tendencies - for adapting the suitable type of authentication to the specific situation [12]. According to [12], there are three ways that adaptive authentication can be deployed:

1. The system admin can define fixed risk levels based on static policies for different factors, such as user's location, authentication's request time of day, day of week, user role, or resource importance.
2. The system can observe the user's typical day-to-day activities on his/her habits and tendencies over time and generate proper dynamic policies. This

learning process of adaptive authentication is similar to behavioral correlation [12].

3. A combination of both 1 and 2 ways utilizing static and dynamic policies.

Regardless of how the risk levels are defined for certain application, the main idea is that adaptive authentication adapts to that risk level, enabling the appropriate level of authentication for the given level of risk [12], [14]. For instance, when a land and sea border control officer is using the mobile passenger ID device in their usual shift (i.e., the date and time of the day that they are supposed to be working), re-authentication should not be required (e.g., the risk level is low). While in case of device usage at any other time (e.g., high risk level), the service may lock, and its unlocking may be only possible by IT staff. Or, when an officer is located in a nonverified location during their shift (e.g., medium risk level), the system should require additional evidence that this person is who claims to be by asking re-authentication.

Adaptive authentication enables significant benefits for user authentication for the mobile passenger identification devices used by border control officers at land and sea borders. In particular, adaptive authentication can ensure that certain attributes about the land and sea border control officer will be monitored and changes on these attributes will enable different authentication methods. In this way, officer's activities will not be interrupted for inessential reasons, while additional authentication will be required only when the risk level has reached a particular value. It is worthwhile to highlight that proper attributes, also refer to as fraud indicators [15], [16], about the land and sea border control officer should be considered in order to design and develop effective and efficient adaptive authentication. In Section III, the design of the proposed mechanism is presented in detail.

B. Risk-Based Authentication

In [12], the authors describe risk-based authentication as the continuous decision on user authentication acceptance or rejection based on the user's behavior and the risk of his action. In particular, this decision depends on the comparison of a risk score computed in real time with the stored risk profiles of the users, and, when required, the system challenges the users for reauthentication, accordingly. Nowadays, risk-based authentication schemes have been attractive among the researchers in this field, offering frictionless user authentication while enhancing security and promoting user's comfort [12], [17]–[19].

The most challenging part when designing and implementing risk-based authentication mechanisms is the technology based on which the risk-based authentication mechanisms define the risk score [12], [16], [20]. An effective and efficient risk-based authentication solution will build the risk score based on the combination of user's contextual information such as user's location, date, time, device's ID, and device's connection, as well as other factors including the device attributes, the user history, the user's behavioral patterns, etc. This combination will ensure a more reliable and rigorous risk score with a minimal interruption to the user's experience and officer's missions.

There is no doubt that the risk estimation component constitutes a key part of the risk-based authentication mechanisms as it is the responsible element for processing available information from user's environment (e.g., contextual information) and user's profile (e.g., user risk history reflecting previous user's behavior patterns), to calculate a risk score associated to the user's current activity [21]. Generally, different methodologies have been proposed over the years for estimating the risk score of an action or event [22]. Risk Assessment (RA) is a well-established qualitative approach within information security for ensuring a commensurate level of security is provided given the risks [23]. The authors in [23] developed a Mobile Device Risk Assessment (MDRA) based on the traditional RA, in which they constructed the Risk Matrix based on Threat Level and Asset Value, evaluating the risks associated with various actions and applications in a mobile device in a user-friendly manner. Although existing qualitative approaches sound reasonable, they involve a lot of expert intuition, and thus the risks are always rated subjectively, making this approach an unsuitable solution for real-world scenarios and sensitive applications such as public safety [24], [25]. Thus, in practical cybersecurity cases, there is the tendency to move in the direction of more quantitative risk assessment methods in order to measurably improve risk assessments [24]. Towards this direction, effort should be placed on developing and implementing novel and efficient quantitative security risk estimation algorithms, suitable for sensitive applications. In the literature, various classification algorithms, such as decision trees [26]–[29], Naïve Bayes [16], [27], logistic regression [24], [27], etc. and other approaches, such as fuzzy logic [26], [30], [31] and Monte Carlo simulation [26], [32] have been proposed for quantitative risk estimation. The efficiency and effectiveness of these approaches are evaluated based on their performance to accurately classify a risk score of an action or an event which requires a comprehensive dataset that contains user's normal and abnormal behaviors. One of the major research challenges in this field is the lack of this kind of datasets. To the best of our knowledge, HuMldb dataset, described in II.C, is one of the few publicly available datasets for behavioral user authentication.

C. HuMldb for Behavioral User Authentication

The HuMldb dataset (Human Mobile Interaction database) includes data captured by 14 sensors (i.e., Accelerometer, L.Accelerometer, Gyroscope, Magnetometer, Orientation, Proximity, Gravity, Light, TouchScreen, Keystroke, GPS, WiFi, Bluetooth, and Microphone), during natural human-mobile interaction performed by more than 600 smartphone users [33], [34]. For the data acquisition, the authors developed an Android application that gathers sensor signals when users perform eight effortless tasks with their own devices and without any supervision whatsoever (i.e., the users could be walking, sitting standing, at daytime or night, being indoors or outdoors, etc.). In particular, the designed tasks included: a) keystroking, b) swipe up, c) tap and double tap, d) swipe down, e) circle hand gesture, f) cross hand gesture, g) voice, and h) finger handwriting. The acquisition protocol comprised 5 sessions with at least 1 day gap among them (i.e., the minimum time between one user finishes a session and the next time the app allows to have

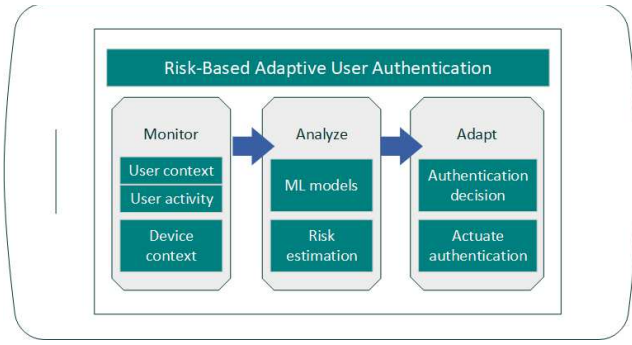


Figure 1: The architecture of the proposed Risk-Based Adaptive User Authentication mechanism.

the next session). At the beginning of each task, the app shows a brief pop-up message explaining the procedure to complete each task. The application also captured the orientation (e.g., landscape/portrait) of the smartphone, the screen size, resolution, the model of the device, and the date when the session was captured. The developed app was advertised in the authors' research web site and was launched on Google Play Store. Afterwards, participants were self-selected worldwide, producing a diverse network of people compared to previous state-of-the-art mobile databases. The authors in [33], [34] highlight that all captured data have been stored in private servers and anonymized with previous participant consent according to the GDPR (General Data Protection Regulation).

The structure of HuMldb is as follows:

User → Sessions → Tasks → Sensors

where the data are stored in nested folders with the ID number to identify each user's folder. Inside the user's folder, there are five folders corresponding to the different sessions the user has completed and three CSV files with the Bluetooth, WiFi and GPS data signals acquired during the entire session. Finally, in each session there are folders for each task that contains data from all sensors required for the particular task.

In [34], Acien et al. used the heterogeneous flow of data generated during the human interaction with smartphone devices to model user's behavior for user authentication purposes. On top of that, they trained their machine learning models with the HuMldb database and they explored the possibility of improving bot detection using smartphone sensors. In addition, they evaluated their proposed CAPTCHA method using fake samples synthesized by Generative Adversarial Neural Networks and handcrafted methods. Their results were promising, suggesting the potential of mobile sensors to characterize the human behavior authenticating the legitimate users.

III. PROPOSED RISK-BASED ADAPTIVE USER AUTHENTICATION MECHANISM

The proposed Risk-Based Adaptive User Authentication mechanism comprises a novel secure and usable authentication solution ensuring continuous authentication behind-the-scenes and invisible to the user (i.e., border control officer). Particularly, its main objective is to automatically adapt the authentication requirements and the suitable type of authentication to the specific situation based

on a real-time risk score depending on the combination of: i) the user's contextual information such as user's location, date, time, device's ID, and device's connection, ii) the user's behavioral patterns, and iii) device context.

A. Mechanism Architecture

In this section, we propose the overall design architecture of the proposed risk-based adaptive user authentication mechanism, as depicted in Fig. 1, presenting in detail its main processes: (a) monitor, (b) analyze and (c) adapt.

- **Monitor:** This module gathers data from the device's sensors about the user context and activity as well as the device context in order to create the user profile (e.g., the user's geographical location, time, and behavioural patterns) and the device profile (e.g., IP addresses and network reputations about the network to which the device is connected), respectively, that uniquely corresponds to a legitimate user accessing a particular mobile device. It follows an event driven approach in which the data collection is only happening when the user performs an action or activity, minimizing the consumed resources.
- **Analyze:** This module receives the data (i.e., event driven approach) from the monitored features and estimates a risk score, using machine learning algorithms, which corresponds to the user's current context and activity as well as the device's current context which is then utilized to adapt – if needed - the authentication requirements and type. The risk score is used to indicate the level of the risk, namely low, medium or high risk. Once the risk level is established, decision will be made in the Adapt component.
- **Adapt:** This module adapts to suitable authentication type given the risk score calculated in the Analyze component. If the risk score is low, no further action would be needed, while if it is medium, additional evidence about the identity of the user may be required and thus asking for re-authentication. In case that the risk score is high, the mobile device may be locked. The last step in this stage is the implementation of the authentication decision.

B. Mechanism Components

The key components of the proposed Risk-Based Adaptive User Authentication mechanism are the following:

- 1) **Risk Estimation Agent (REA):** The risk estimation agent makes use of the user profile and the device profile to estimate the overall real-time risk score the first time that the officer attempts to get authenticated and sign in as well as every time that the user profile is updated from the user context monitoring component.
- 2) **Risk Policies (RPs):** Regulations that specify the correct or expected behavior of an officer within the certain context of border control environment, established by the administration. In particular, RPs include: a) information about the officer shifts (i.e., the specific geographical location and time that every officer is expected to be working); b) network information (i.e., IP addresses and network reputations) about the network to which the mobile devices are expected to be connected to; c) the registered

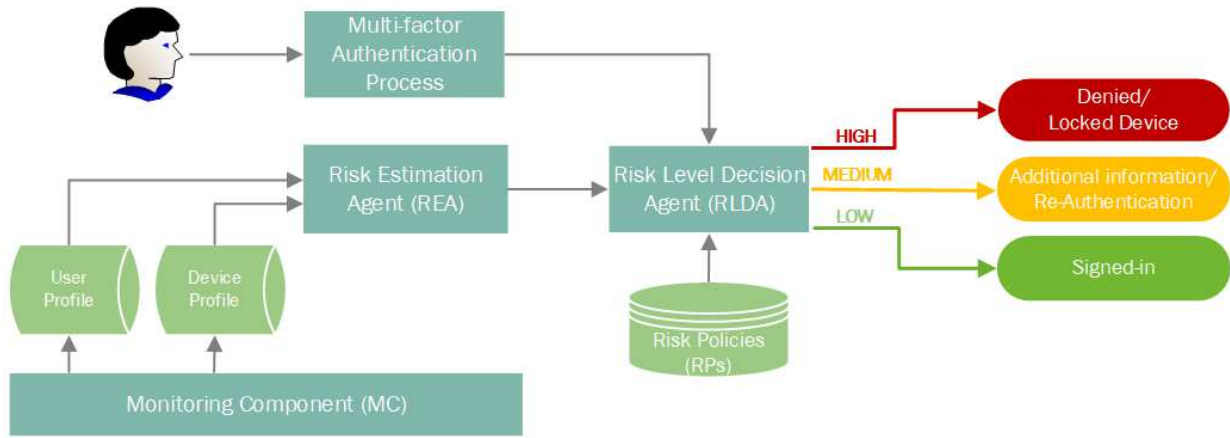


Figure 2: The generic flow of the proposed Risk-Based Adaptive User Authentication mechanism.

device(s) to which the requested officer is expected to be assigned with; and d) the expected closeness to the user's proximity token. The RPs are essential for setting the threshold values for the risk score estimated by REA. The set threshold values are applied by RLDA in order to make a decision (i.e., whether a risk score is low, medium, or high).

3) **Risk Level Decision Agent (RLDA):** The estimated risk score is compared with the risk level thresholds, set by the corresponding RPs, to classify whether the estimated risk score is low, medium, or high.

4) **First-time Authentication:** During the first time-authentication, the officer is being authenticated through a two-level authentication process. At the first level, the officer is being authenticated through a multi-factor authentication process based on a PIN and a proximity token). In case that the validity of the claimed identity of the officer requesting access to the device is verified, the first-level authentication is considered as successful and then, the second level of authentication takes place. Otherwise, the authentication request is denied and the authentication process stops. In the second level, the first-level authenticated request is forwarded to RLDA which is responsible for the second-level authentication based on the overall real-time risk score calculated by REA. Depending on the decision taken by RLDA the officer may be: (i) allowed to sign-in when the risk level is low; (ii) required to provide additional authentication information (i.e., something that he/she has such as iris-based authentication) when the risk level is medium; or (iii) denied to sign-in when the risk level is high.

5) **Re-authentication:** Once the officer is signed in and throughout their login session, REA receives updated data from the monitored features stored in the user profile and device profile, every time that the user performs an action or activity, and estimates a risk score, using machine learning algorithms, which corresponds to the user's current context and activity as well as the device's current context. Afterwards, the estimated risk score is forwarded to RLDA which takes decision about the re-authentication based on the risk score. In case that the risk score is medium, re-authentication will be required in order the officer to provide additional information whether he/she is authorised or not to utilize the mobile device. Physiological biometrics have been widely proposed and utilized for precise and

convenient user authentication. Despite that they are considered secure due to the fact that they uniquely identify a user, many of them have shown to be vulnerable to security attacks such as impersonation. In particular, malicious actors have successfully managed to trick face recognition and fingerprint in mobile devices, with photos of the face or the finger (from the peace symbol) of the legitimate user obtained from social media [35]–[38]. However, iris-based authentication, which identifies patterns within an individual's iris to uniquely identify an individual, has been identified in the literature as one of the most effective and efficient biometrics, that it is almost impossible to hack [11]. According to a new report from the National Institute of Standards & Technology (NIST), iris recognition technology used to identify an individual from a crowd is accurate 90 percent to 99 percent of the time [11]. Iris-based authentication whose complex patterns are unique, stable, and can be seen from some distance is being considered one of the most accurate biometric authentication methods. On top of that, it has the advantages of being contactless and no user's previous knowledge is required. Therefore, it constitutes a feasible module for implementing the re-authentication in our proposed risk-based adaptive user authentication mechanism.

6) **Monitoring Component (MC):** Once officer's first-time authentication is successful and throughout their login session, the Monitoring Component, behind-the-scenes and without interrupting officer's normal activities and missions, continuously monitors: a) the officer's contextual information (i.e., the officer's geographical, location, time, and information about the closeness to the user's proximity token); b) the officer's activity (i.e., behavioural patterns); and c) the device's contextual information (i.e., IP addresses and network reputations). If the MC detects any changes regarding these attributes, it updates the user profile and the device profile.

IV. CONCLUSIONS

Novel secure and usable user authentication mechanisms are required to increase the level of security of new mobile devices for passenger identification used by border control officers at land and sea borders, without interrupting border control activities. Towards this direction, we discuss background concepts on adaptive and risk-based authentication and a review of related work on

user authentication solutions for mobile devices is given in order to provide a foundation for organizing research efforts towards the design and development of effective and efficient risk-based adaptive user authentication for mobile passenger identification devices used by border control officers at land and sea borders. Besides that, a novel risk-based adaptive user authentication mechanism is proposed. Our next steps include the implementation of quantitative risk estimation approaches to identify the most effective and efficient ones for risk-based adaptive user authentication mechanisms on the mobile devices for passenger identification at land and sea borders.

REFERENCES

- [1] B. Jakobsen, B. T. Muguruza, D. C. de Magalhaes, A. Ballester, and M. Sweerts, "Challenges to effective EU cybersecurity policy - Briefing Paper," *Eur. Court Audit.*, no. March, pp. 1–74, 2019.
- [2] World Economic Forum, *The Global Risks Report 2021: 16th Edition*. 2021.
- [3] European Commission, "Mobility and Transport Transport in the European Union Current Trends and Issues BACKGROUND INFORMATION," *Eur. Comm.*, no. April, p. 144, 2018.
- [4] M. Papaioannou, G. Mantas, D. Lymberopoulos, and J. Rodriguez, "User Authentication and Authorization for Next Generation Mobile Passenger ID Devices for Land and Sea Border Control," *2020 12th Int. Symp. Commun. Syst. Networks Digit. Signal Process. CSNDSP 2020*, pp. 8–13, 2020.
- [5] J. Ribeiro, F. B. Saghezchi, G. Mantas, J. Rodriguez, S. J. Shepherd, and R. A. Abd-Alhameed, "An Autonomous Host-based Intrusion Detection System for Android Mobile Devices," *ACM/Springer Mob. Networks Appl.*
- [6] G. Mantas, N. Komninos, J. Rodriguez, E. Logota, and H. Marques, "Security for 5G Communications," in *Fundamentals of 5G Mobile Networks*, J. Rodriguez, L. Eds., John Wiley & Sons, Ed. Chichester, UK, 2015, pp. 207–220.
- [7] M. Papaioannou et al., "A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT)," *Trans. Emerg. Telecommun. Technol.*, no. May, pp. 1–15, 2020.
- [8] I. Essop, J. C. Ribeiro, M. Papaioannou, J. Rodriguez, G. Zachos, and G. Mantas, "Generating datasets for anomaly-based intrusion detection systems in iot and industrial iot networks," *Sensors*, vol. 21, no. 4, pp. 1–31, 2021.
- [9] F. P. Oikonomou, J. Ribeiro, G. Mantas, J. Bastos, and J. Rodriguez, "A Hyperledger Fabric-based Blockchain Architecture to Secure IoT-based Health Monitoring Systems," in *2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom) Work Acc.*
- [10] M. Papaioannou, G. Mantas, and J. Rodriguez, "Risk-Based User Authentication for Mobile Passenger ID Devices for Land and Sea Border Control," in *2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom) Work Acc.*
- [11] Y.-Y. Choong, J. M. Franklin, and K. K. Greene, "Usability and Security Considerations for Public Safety Mobile Authentication," *Natl. Inst. Stand. Technol. Interag. Rep. 8080*, 2016.
- [12] S. Gupta, A. Buriro, and B. Crispo, "Demystifying Authentication Concepts in Smartphones: Ways and Types to Secure Access," *Hindawi Mob. Inf. Syst.*, vol. 2018, 2018.
- [13] V. M. Patel, R. Chellappa, D. Chandra, and B. Barbello, "Continuous User Authentication on Mobile Devices: Recent progress and remaining challenges," *IEEE Signal Process. Mag.*, vol. 33, no. 4, pp. 49–61, 2016.
- [14] "Identity Automation, 'Risk-based authentication,'" <https://www.identityautomation.com/iam-platform/rapididentityidentityaccess-management/multi-factor-authentication/risk-basedauthentication/>, 2017.
- [15] A. Hurkala and J. Hurkala, "Architecture of Context-Risk-Aware Authentication System for Web Environments," *Icicis'2014*, pp. 219–228, 2014.
- [16] EMC, "The RSA Risk Engine," 2015.
- [17] A. J. Harris and D. C. Yen, "Biometric authentication: Assuring access to information," *Inf. Manag. Comput. Secur.*, vol. 10, no. 1, pp. 12–19, 2002.
- [18] I. Traore, I. Woungang, M. S. Obaidat, Y. Nakkabi, and I. Lai, "Online risk-based authentication using behavioral biometrics," *Multimed. Tools Appl.*, vol. 71, no. 2, pp. 575–605, 2014.
- [19] B. Causey, "Adaptive authentication: an introduction to riskbased authentication," 2013.
- [20] Spooeren Jan, Davy Preuveneers, and Wouter Joosen, "Mobile device fingerprinting considered harmful for risk-based authentication," *Proc. Eighth Eur. Work. Syst. Secur.*, 2015.
- [21] M. T. Gebrie and H. Abie, "Risk-based adaptive authentication for internet of things in smart home eHealth," *ACM Int. Conf. Proceeding Ser.*, vol. Part F1305, pp. 102–108, 2017.
- [22] W. A. Jansen, T. Winograd, and K. Scarfone, "Guidelines on Active Content and Mobile Code," *Recommendations of the National Institute of Standards and Technology*, 2008. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublicatio n800-28ver2.pdf>.
- [23] T. Lederm and N. L. Clarke, "Risk assessment for mobile devices," in *International Conference on Trust, Privacy and Security in Digital Business*, pp. 210–221.
- [24] D. W. Hubbard and R. Seiersen, *How to Measure Anything in Cybersecurity Risk*. Wiley, 2016.
- [25] M. Ghazouani, S. Faris, H. Medromi, and A. Sayouti, "Information Security Risk Assessment A Practical Approach with a Mathematical Formulation of Risk," *Int. J. Comput. Appl.*, vol. 103, no. 8, pp. 36–42, 2014.
- [26] H. F. Atlam, A. Alenezi, R. J. Walters, and G. B. Wills, "An overview of risk estimation techniques in risk-based access control for the internet of things," *IoTBDs 2017 - Proc. 2nd Int. Conf. Internet Things, Big Data Secur.*, no. April, pp. 254–260, 2017.
- [27] M. Heydari, A. Mylonas, V. Katos, E. Balaguer-Ballester, V. H. F. Tafreshi, and E. Benkhelifa, "Uncertainty-aware authentication model for fog computing in IoT," in *Fourth International Conference on Fog and Mobile Edge Computing (FMEC)*, 2019, pp. 52–59.
- [28] K. Shang and Z. Hossen, "Applying Fuzzy Logic to Risk Assessment and Decision-Making," *Casualty Actuarial Society, Canadian Institute of Actuaries, Society of Actuaries*, 2013. [Online]. Available: <https://www.soa.org/globalassets/assets/Files/Research/Projects/research-2013-fuzzy-logic.pdf>.
- [29] S. Wang, C. Fan, C.-H. Hsu, Q. Sun, and Y. Fangchun, "A Vertical Handoff Method via Self- Selection Decision Tree for Internet of Vehicles," *IEEE Syst. Journal*, 10(3), pp. 1183–1192, 2016.
- [30] M. Friedman and A. Kandel, "On the design of a fuzzy intelligent differential equation solver," in *Fuzzy Expert Systems*, 1992, pp. 203–212.
- [31] L. A. Zadeh, "On fuzzy algorithms," in *In fuzzy sets, fuzzy logic, and fuzzy systems: selected papers By Lotfi A Zadeh*, 1996, pp. 127–147.
- [32] S. A. Goerdin and R. P. Smit, J.J. and Mehairjan, "Monte Carlo simulation applied to support risk-based decision making in electricity distribution networks," in *2015 IEEE Eindhoven PowerTech*, 2015, pp. 1–5.
- [33] A. Acién, A. Morales, J. Fierrez, R. Vera-Rodriguez, and I. Bartolome, "BeCAPTCHA: Detecting Human Behavior in Smartphone Interaction using Multiple Inbuilt Sensors," 2020.
- [34] A. Acién, A. Morales, J. Fierrez, R. Vera-Rodriguez, and O. Delgado-Mohatar, "BeCAPTCHA: Bot Detection in Smartphone Interaction using Touchscreen Biometrics and Mobile Sensors," no. May, 2020.
- [35] J. Titcomb, "Hackers claim to beat iPhone X's face id in one week with 115 mask," 2017.
- [36] S. Kovach, "Business insider-Samsung's Galaxy S8 facial recognition feature can be fooled with a photo," 2017.
- [37] A. Charles, "The guardian-iPhone 5S fingerprint sensor hacked by Germany's Chaos Computer Club," 2013.
- [38] D. McGoogan, C., & Demetriou, "Peace sign selfies could let hackers copy your fingerprints," 2017.