Risk-Based User Authentication for Mobile Passenger ID Devices for Land and 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

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

***Abstract*—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 promote further the comfort of passengers. Nevertheless, the highly sensitive information handled by this type of devices makes them an attractive target for malicious actors. 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 authentication for mobile devices as a suitable approach to deal with the security vs. usability challenge. Besides that, an overview of existing risk estimation approaches – both qualitative and quantitative – is given to provide a foundation for organizing research efforts towards the design and development of proper risk estimation mechanisms for risk-based user authentication for mobile passenger identification devices used by border control officers at land and sea borders.**

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

I. INTRODUCTION

According to the European Commission [1], transport is a fundamental sector for and of the world economy comprising a diverse and complex network of around 1.2 million enterprises across the EU, employing virtually 11 million individuals and delivering products and services to EU residents, companies and its trading partners. In order to exploit the economic strengths of the EU, and to empower cohesion both at economic and social level, efficient transport services and infrastructure comprise a cornerstone component. While airports are of an acceptable standard, land border crossing points and sea ports require more research and investment for novel efficient solutions, such as mobile passenger identification devices for land and sea border control for accurate passenger identification "on the fly" while ensuring passenger´s comfort [2].

Nevertheless, the highly sensitive and confidential information handled by these devices makes them an attractive target for malicious actors in terms of data loss, data theft and data misuse [2], [3]. In order to ensure high level of device security to protect sensitive data handled by these devices, strong user authentication mechanisms are required [4], [5], [6]. Due to the fact that 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. According to NIST Special Publication 8080 [7], 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 (such as the land and sea border control officers). Therefore, it is of utmost importance the design and implementation of novel secure and usable user authentication mechanisms that will increase the level of security of the passenger identification mobile devices and will ensure that border control officers at land and sea borders are able to successfully complete their missions [2].

However, security and usability are often thought of as being contradictive [2]. To deal with this security vs. usability challenge, risk-based type of user authentication mechanisms has been proposed to dynamically authenticate a legitimate user throughout his entire interaction with the mobile device, based on a risk score computed in real-time, enhancing the reliability of whole authentication process without interrupting the user's normal activity (i.e., the land and sea border control officers on the field) [8]. The risk estimation component plays a key role in the design and implementation of proper secure and usable risk-based user authentication mechanisms, and in order to ensure a precise risk score computation, more sophisticated risk estimation algorithms must be studied and implemented.

Towards this direction, we, firstly, discuss background concepts on risk-based authentication and a review of related work on user authentication solutions for mobile devices. Besides that, an overview of existing risk estimation approaches – both qualitative and quantitative – is given in order to provide a foundation for organizing research efforts towards the design and development of proper risk estimation mechanisms for risk-based user authentication for mobile passenger identification devices used by border control officers at land and sea borders.

Following the Introduction, the rest of the paper is organized as follows. Section II presents risk-based user authentication and a review of related work on user

authentication solutions for mobile devices. In Section III, an overview of existing qualitative and quantitative risk estimation approaches is provided. Finally, the paper is concluded in Section IV.

II. Risk-Based User Authentication

According to review article [8], risk-based authentication schemes are based on a continuous decision to accept or reject user authentication by monitoring the user's behavior and the risk of his/her action, as depicted in Fig. 1. This decision depends on the comparison of a risk score computed in real time with the stored risk profiles of the users, and then the system challenges the users for re-authentication, accordingly. For instance, when an officer is using the mobile identification device from a verified secure location (land or sea border control workplace), re-authentication should not be required. While in case of an unknown or nonverified location, the service may require additional evidence about the identity of the user and thus asking for re-authentication. Nowadays, risk-based authentication schemes tend to offer frictionless user authentication while enhancing security and promoting user´s comfort [8], [9], [10], [11]. Although many security companies offer risk-based authentication for mobile devices, the difference on whether a mechanism is efficient or not lies in the technology that the risk-based authentication scheme uses to determine the risk score: the risk estimation scheme [12], [13]. An effective risk-based authentication solution will not only build a risk score based only on contextual user information (e.g., device´s ID, location, date, time, and connection) but will also make use of the user's behavioral patterns [14], [15], the device attributes, the user history, and other factors to make the score accurate and reliable while ensuring minimal interruption to the user´s experience. On top of that, it is of utmost importance to implement risk estimation algorithms to efficiently quantify the risk score. 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 [16], [17]. Finally, risk-based user authentication can be applied from two different perspectives: proactive or re-active [8]. In the first case, risk-based authentication scheme actively anticipates the genesis of potential attacks, failures, or any kind of security issues and takes prompt action. While re-active risk-based authentication accepts some of the risks until the risk score goes beyond the acceptable threshold level, and consequently, reauthentication is required.

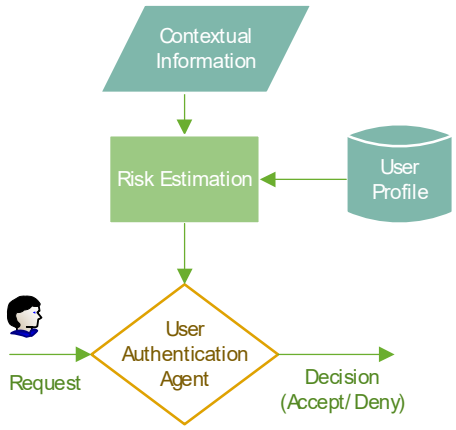

Figure 1: Risk-based user authentication overview.

TABLE I.

Fraud Indicators
User IP address
Time of access
Device cookie
Device profiling
Number of failed authentication attempts

In [18], Hintze et al. evaluate the risk and make authentication decision for mobile devices based on user´s geographical location and multi-modal biometrics. On the other hand, in [19], Hurkala et al. proposed a context risk aware authentication to evaluate the risk associated to the user identity. In particular, the authors used both provided and observed information about the user to create a user profile and measure the probability that an attacker is trying to impersonate the user during authentication request based on this user profile. On top of that, to evaluate the risk associated with an authentication request, they analyzed circumstances surrounding the login attempt and the history of previous login attempts. The circumstances used in their model, also referred to as fraud indicators are shown in TABLE I. It is crucial to use as many fraud indicators as possible to achieve a more accurate risk estimation. Gascon et al. in [20] considered the evaluation of fingerprint movement for learning the behavior of the smartphone user to transparently authenticate the user in an ongoing-fashion. The authors used all available mobile sensors to determine a typing motion fingerprint of the user. After the proper feature extraction, a machine learning classifier based on Support Vector Machines (SVM) was used to identify the legitimate user. The results of their study were twofold: While their approach was able to continuously authenticate some users with high precision, there also were participants for which no accurate motion fingerprint could be learned.

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, risk estimation follows an event driven approach in which the risk score is only estimated when an abnormality on a set of attributes has been detected, which minimizes the consumed resources [8]. In the following, an overview of existing qualitative and quantitative risk estimation approaches is given in order to provide a foundation for organizing research efforts towards the design and development of proper risk estimation for risk-based user authentication for mobile passenger identification devices used by border control officers at land and sea borders.

III. Risk Estimation

Different methodologies have been proposed over the years for estimating the risk score of an action or event. According to NIST SP 800-28 v2 [22], risk is ``*a measure of the likelihood and the consequence of events or acts that could cause a system compromise, including the unauthorized disclosure, destruction, removal, modification, or interruption of system assets*´´. In general,

			Impact				
			Negligible	Minor	Moderate	Critical	Catastrophic
			1	2	3	4	5
Likelihood	Frequent	5	Medium	Medium	High	High	High
	Likely	4	Medium	Medium	Medium	High	High
	Occasional	3	Low	Medium	Medium	Medium	High
	Seldom	2	Low	Low	Medium	Medium	Medium
	Improbable	1	Low	Low	Low	Medium	Medium

Figure 2: The traditional RA risk matrix [16].

the risk estimation process can be qualitative or quantitative [23]. Qualitative assessment includes the use of a set of methods, principles, or rules for assessing risk based on nonnumerical categories or levels [23]. On the other hand, the quantitative assessment refers to the use of a set of methods, principles, or rules for assessing risks based on the use of numbers where the meanings and proportionality of values are maintained inside and outside the context of the assessment [23].

A. Qualitative approach

Risk Assessment (RA) is a well-established qualitative approach within information security for ensuring a commensurate level of security is provided given the risks [24]. As such, various information security standards were developed such as, ISO/IEC 27000 standards and the National Institute of Standards and Technologies Special Publication 800 Series [24]. Nowadays, the majority of businesses and enterprises perform regularly qualitative risk assessment for identifying, estimating, and prioritizing risks to organizational operations, including mission, functions, image, reputation, organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system (NIST SP 800-30 Rev. 1 under Risk Assessment NIST SP 800-39) [25]. Typically, in a qualitative risk assessment performed in enterprises, the risk score is a function of (i) the adverse impacts that would arise if the circumstance or event occurs and (ii) the likelihood of occurrence ([23] under Risk CNSSI 4009), and the most common mathematical formula to represent it in quantitative term is:

$$Risk\ Score = Likelihood \times Impact \quad (1)$$

		Asset value							
		1	2	3	4	5	6	7	8
Threat level	1	1	1	2	3	4	5	6	7
	2	1	1	2	3	4	5	6	7
	3	1	2	3	4	5	6	7	8
	4	2	3	4	5	6	7	8	8
	5	2	3	4	5	6	7	8	8

Figure 3: The MDRA risk matrix [24].

where likelihood represents the probability of an incident to happen, and impact represents the estimation of the value of the damage regarding that incident ([23] under Risk CNSSI 4009). Then, based on the results of the risk estimation process, the estimated risk scores are transformed into a "human readable" format. This allowed us to categorize each risk into buckets of HIGH, MEDIUM, and LOW, as illustrated in Fig. 2.

The authors in [24] developed a Mobile Device Risk Assessment (MDRA) based on the traditional RA. Their risk calculation scheme consists of the six steps as shown in TABLE II. The authors considered assets the installed applications and services in the mobile device such as e-mail, e-banking, e-health, stored sensitive documents, and they assessed an asset value (from 1 to 8) in each asset based on the applications sensitivity. In addition, they considered threat levels from 1 (less severe) to 5 (harmful), and they constructed a Risk Matrix based on Threat Level and Asset Value, as shown in Fig. 3. Their main goal was to evaluate the risks associated with various actions and applications in a mobile device in a user-friendly manner.

TABLE II.

MDRA Step	Description
1	Evaluation of asset value categories
2	Calculation of a single asset value
3	Evaluation of threats
4	Calculation of a single threat value
5	Answer vulnerability questions
6	Calculation of risk level

Nevertheless, in one widely used approach, “likelihood” and “impact”, or “threat level” and “asset value” involves a lot of expert intuition and thus, they will be rated subjectively, perhaps on a 1 to 5 scale, creating a “risk matrix” —similar to the one shown in Fig. 2 and Fig. 3 [16]. More precisely, actions or events with both high likelihood and high impact would be considered “high risk” (i.e., upper-right corner), while those with low likelihood and low impact would be in the opposite considered “low risk” events (i.e., upper-left corner), as depicted in Fig.2. The main idea is that the higher the score, the more important something is and the sooner you should address it. Although this approach may sound totally reasonable, 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 [16].

B. Quantitative approach

Many risk analysts believe that even though giant breaches such as Target, Anthem, and Sony have already occurred, “The Big One” has not happened yet [16]. On top of that, although breaches are - de facto - unpredictable events, an efficient risk estimation algorithm can give invaluable insight into the potential risks and the intelligence to help mitigate this kind of risks [16]. However, as we cited before, effort should be placed on developing and implementing novel and efficient quantitative security risk estimation algorithms, suitable for sensitive applications. In the following, the major classification algorithms and other

methodologies identified in the literature for quantitative risk estimation are presented.

1) Machine Learning Classification Algorithms

a) Decision tree

Decision tree is a supervised classification algorithm that performs hierarchical decision making on the feature values based on a set of rules presented in a tree-like structure [26], [27]. As in all machine learning algorithms, firstly, data are divided into training and validation data sets. Training data are used to identify proper set of rules and the optimal partition for certain attributes using techniques such as recursive partitioning. In particular, any decision made divides the tree based on a criterion in a way that the training data is split into two or more branches. The main objective is to find the optimal split criterion so as the number of mixing the class variables in each branch of the tree is reduced as much as possible [27]. Afterwards, validation data are used to validate the decision tree and make necessary adjustments to the tree in order to make it more efficient [26], [28].

Reference [27] reports that there are three classical algorithms for implementing a decision tree: ID3, C4.5 and CART (Classification and Regression Trees). These algorithms employ 'Entropy' and 'Gini' as splitting criteria [27]. However, since the desired output of their system is the binary decision: *Accept* or *Deny* authentication, the authors in [27], among the three aforementioned classical algorithms for decision tree, applied the CART classification algorithm in order to build their data model. They also constructed a dataset on Matlab, based on the state-of-the-art research, to develop their data-driven model (i.e., classifier). CART shows benefits over the other algorithms in terms of reducing over-fitting and the ability of handling incomplete data [27]. On top of that, it is able to build models for regression as well as classification. CART employs Gini criterion for splitting the training data. An optimized version of CART implemented in scikit-learn is presented in [27].

The main advantage of decision tree is that it works well even with insufficient data if proper set of rules is determined by security experts. However, in a typical decision tree model, the partition of feature values is based on classical set theory. Furthermore, a slight change in certain value of an attribute could lead to a totally different conclusion because of the discreteness of the partition. Decision trees are considered valuable models for classification and easy to understand [26], [28]. However, when the decision tree becomes significant in terms of size, it becomes more difficult to understand it and, in addition, more data are needed for identifying and validating the set of rules [26], [28], [29].

TABLE III.

Fraud Indicators
Activity type (e.g., login, payment, password change)
User details including name, language, country, etc.
Device details including IP address, browser characteristics, screen resolution, etc.
Mobile device details including mobile sim id, mobile geo location, wifi MAC address, etc
User interactions with the device such as mouse movements and key strokes
Payment details such as the amount, currency, and the payee account
Indicators of Trojan malware activities

b) Naïve bayes

Naïve Bayes classifier constitutes the simplest form of a bayesian Network. The term 'naïve' arises from the fact that this algorithm considers all the attributes conditionally independent in order to simplify the process of modelling. Regardless this controversial assumption, it is anticipated that Naïve Bayes is a fast classifier and has a great performance in practice for many domains [27]. The authors in [27] applied Gaussian Naïve Bayes classifier implemented in the scikit-learn library for their proposed a novel prediction model with binary decision: *Accept* or *Deny* authentication. According to their findings, Naïve Bayes model showed lower performance with respect to true positive and false positive rates than the other used prediction models, namely Decision Tree, Logistic Regression and Support Vector Machine.

Furthermore, the RSA Risk Engine (RE) is used to analyze a wide range of indicators and attributes associated with an activity in a mobile device, as shown in TABLE III., to determine the probability that the activity is fraudulent [13]. In particular, the RE combines Bayesian machine learning methods with sophisticated device identification and recognition and user behavior analysis to enable intelligent decisioning that significantly reduces fraud.

c) k-NN

The k-NN is a supervised machine learning technique which can be used for estimation, prediction, pattern recognition, and classification. It totally relies on instance-based learning, in which a range of training data is saved for the purpose of finding out the class type of new unclassified data. k-NN algorithm has been detected by many researchers, most especially Lloyd (1957, 1982), Forgey (1965), Friedman and Rubin (1967), and McQueen (1967).

More precisely, Instance-Based Learning (IBL) classifiers such as the k-NN algorithm classify similar instances under the same class labels. To achieve this, they determine the closest K training samples, and select the dominant class label among them as the relevant class [30]. The authors in [30] proposed a location-aware model, in which they calculated a risk score based on changes in the location, and then, they classified this risk score using the k-NN classifier to accept or deny the authentication. According to their findings, the k-NN classifier presents a significant advantage in terms of its simplicity. On top of that, it is noise-tolerant, and it has relatively low update cost [30]. Finally, they applied all three IBL algorithms from scikit-learn namely as 'Brute Force', 'K-D Tree' and 'Ball Tree' in order to build their prediction model and compare the performance results.

d) Logistic regression

Logistic regression is an analytic method used in classification problems for modeling and classifying

scenarios with two or more possible discrete outcomes [27]. In the risk estimation process, it might be suitable for classifying the risk score as low, medium, or high. Logistic regression applies a probabilistic classifier and maps the feature variables to a class-membership probability. Typically, logistic regression is used for building data-driven models with binary outcomes (e.g. Accept/Deny user authentication). In [16], the authors discuss a variation on "logistic regression" for risk estimation: the log odds ratio (LOR) method. LOR provides a way for an expert to estimate the effects of each condition of the system separately and then add them up to get the probability based on all the conditions for the whole system [16]. However, this method involves the estimation of experts, and thus it cannot be considered subjective. In particular, in the beginning, experts will be asked to identify a list of factors relevant to the particular item they will be estimating, as well as to generate a set of scenarios using a combination of values for each of the factors identified. Afterwards, they will provide relevant estimates for each scenario described. Finally, a logistic regression will be performed using the average of expert estimates as the dependent variable and the inputs provided to the experts as the independent variable. Depending on the input variables used, use of multinomial regression methods may be necessary [16].

It is worthwhile to highlight the results presented in [27]. In particular, the authors built a model using four robust classification algorithms namely, logistic regression, SVM, Naïve Bayes and decision tree, for predicting the risk in user authentication for sensitive applications. The authors developed a dataset based on the findings of the state-of-the-art research to train and test the proposed model. Their results showed that prediction model created by logistics regression has the best performance in terms of accuracy (88.14%) and, at the same time, has the lower computational complexity compared to the other classification algorithms.

e) Support Vector Machine (SVM)

The support vector machine (SVM) is one of the most robust and widely used binary classification algorithms [27]. The main objective of the SVM optimization algorithm is to define the separating hyperplane which maximizes the distance between the closest training samples to the support vectors [27]. In this way, misclassification error is reduced, while the generalization capability for test datasets is maximized. On top of that, when the training set is non-linearly separable as it happens in many real-world scenarios, SVM facilitates the linear separability for the two classes by being combined with the kernel trick to expand the space implicitly [27]. In [27], the authors applied the support-vector classification algorithm from scikit-learn library in order to build their prediction model. According to their results, logistic regression and SVM showed to have better performance in terms of model accuracy in comparison with decision tree. In particular, SVM and logistic regression showed similar results in terms of accuracy, precision, recall and F1, however logistic regression achieves better accuracy. The authors discussed that this was expected due to the optimization method that these two algorithms are employing. In other words, the way of updating the model parameters in logistic regression is equivalent to the way of updating the weights in neural network models [27]. Both algorithms continuously update based on their mistakes in classification.

2) Fuzzy logic

Fuzzy logic is a tool for embedding structured human knowledge into workable algorithms. There are two main types of sets: (i) the 'crisp (or classic) sets', and (ii) the 'fuzzy sets'. For instance, a crisp set can be defined by a membership function as follows:

$$\mu_s(\mathrm{X}) \begin{cases} 1 \; if \; X \in S \\ 0 \; if \; X \in \not S \end{cases} \quad (2)$$

In particular, Function (2) defines the degree of membership to a crisp set S. A function of this type, in crisp sets, is also called characteristic function. On the other hand, fuzzy sets can be used to provide rational and sensible clustering. In fuzzy sets, there is also a degree of membership $\mu_s(\mathrm{X}) \in [0,1]$.

In the case of risk estimation for mobile user authentication, every estimated risk simultaneously belongs to all risk clusters (from lowest risk to highest) with a different degree of membership, so as the characteristic cluster for each prefecture to be the one with the highest value of the membership function $\mu_s(\mathrm{X})$ [26], [31]. In order to generate different cases of Degrees of Membership, a trapezoidal or a triangular membership function can be applied [32].

3) Monte Carlo simulation

The Monte Carlo Simulation (MCS) is a powerful method for risk estimation calculating risk scores of hundreds or thousands of possible scenarios [26]. MCS is a practical, proven solution, and it can be performed on any modern personal computer [16]. In particular, MCS uses a conventional computer to generate a large number of scenarios based on probabilities for inputs [16]. Afterwards, a specific value would be randomly generated for each of the unknown variable's scenario, for each scenario. Then these specific values would go into a formula to compute an output for that single scenario. This process usually goes on for thousands of scenarios.

Therefore, MCS can produce a complete probability distribution associated with risk scores and can provide very realistic results. In the MCS method, the system random behavior is represented by performing a set of experiments on the system in the form of simulations [33]. Although MCS method requires high computing power, it has become increasingly interesting, nowadays, due to the availability of high-speed computers in the market. The main benefit of the MCS is that it can work with large complex systems. Moreover, it can manage the probabilistic behavior of multiple inputs to the system which in the analytical technique are supposed to be constant values [33].

IV. Conclusions and Future Work

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, the objective of this work is two-fold: a) to give researchers a better understanding of risk-based authentication for this kind of mobile devices as a suitable approach to deal with the security vs. usability challenge, and b) to provide a foundation for organizing research

efforts towards the design and development of proper risk estimation mechanisms for risk-based user authentication for this kind of mobile devices.

Our next steps include the implementation of quantitative risk estimation approaches to identify the most effective and efficient ones for risk-based authentication mechanisms on the mobile devices for passenger identification at land and sea borders. On top of that, the integration of adaptive authentication towards a risk-based adaptive user authentication mechanism also comprises a future research work direction.

ACKNOWLEDGMENT

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.

REFERENCES

[1] European Commission, "Mobility and Transport Transport in the European Union Current Trends and Issues BACKGROUND INFORMATION," *Eur. Comm.*, no. April, p. 144, 2018.

[2] 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.

[3] 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.*

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] B. Causey, "'Adaptive authentication: an introduction to riskbased authentication,'" 2013. .

[12] NuData Security, "What is Risk Based Authentication? (KBA)." [Online]. Available: https://nudatasecurity.com/resources/blog/ecommerce/what-is-risk-based-authentication/.

[13] EMC, "The RSA Risk Engine," 2015.

[14] J. Ribeiro, F. B. Saghezchi, G. Mantas, J. Rodriguez, and R. A. Abd-Alhameed, "HIDROID: Prototyping a Behavioral Host-based Intrusion Detection and Prevention System for Android," *IEEE Access*, vol. 8, pp. 23154 – 23168, 2020.

[15] J. Ribeiro, F. B. Saghezchi, G. Mantas, J. Rodriguez, S. J. Shepherd, and R. A. Abd-Alhameed, "Towards an Autonomous Host-based Intrusion Detection System for Android Mobile Devices," in *9th EAI International Conference on Broadband Communications, Networks, and Systems (BROADNETS2018)*, 2018, pp. 139–148.

[16] D. W. Hubbard and R. Seiersen, *How to Measure Anything in Cybersecurity Risk*. Wiley, 2016.

[17] 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.

[18] D. Hintze, S. Scholz, E. Koch, and R. Mayrhofer, "Location-based risk assessment for mobile authentication," *UbiComp 2016 Adjun. - Proc. 2016 ACM Int. Jt. Conf. Pervasive Ubiquitous Comput.*, pp. 85–88, 2016.

[19] A. Hurkala and J. Hurkala, "Architecture of Context-Risk-Aware Authentication System for Web Environments," *Icieis'2014*, pp. 219–228, 2014.

[20] H. Gascon, S. Uellenbeck, C. Wolf, and K. Rieck, "Continuous authentication on mobile devices by analysis of typing motion behavior," *Lect. Notes Informatics (LNI), Proc. - Ser. Gesellschaft fur Inform.*, vol. P-228, pp. 1–12, 2014.

[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/nistspecialpublication800-28ver2.pdf.

[23] R. M. Blank and P. D. Gallagher, "Guide for Conducting Risk Assessments," *NIST Special Publication 800-30 Revision 1*, 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[24] 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.

[25] G. Locke and P. D. Gallagher, "Managing Information Security Risk Organization, Mission, and Information System View," *NIST Special Publication 800-39*, 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf.

[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. Heydari, A. Mylonas, V. Katos, E. Balaguer-Ballester, V. H. F. Tafreshi, and E. Benkhelifa, "A Location-Aware Authentication Model to Handle Uncertainty in IoT," *2019 6th Int. Conf. Internet Things Syst. Manag. Secur. IOTSMS 2019*, pp. 43–50, 2019.

[31] M. Friedman and A. Kandel, "'On the design of a fuzzy intelligent differential equation solver.,'" in *Fuzzy Expert Systems*, 1992, pp. 203–212.

[32] 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.

[33] 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.