Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 2 (2025)

Review and Analysis of Mathematical Approaches for Adaptive Authentication using Machine Learning

Ritu Agrawal[1], Reema Ajmera[2], Ekagra Agrawal[3], Jeevant Singh[4]

[1]Research Scholar, Nirwan University Jaipur India
[2]Professor, Nirwan University, Jaipur, India
[3]Student, B.Tech CSE, Manipal University, Jaipur, India
[4]Student, B.Tech CSE(IoT & IS), Manipal University, Jaipur, India
[1]ritu.agrawal@nirwanuniversity.ac.in, [2]researchajmejra@gmail.com, [3]ekagraagrawal@gmail.com
[4] jeevantprakharsingh2004@gmail.com

Article History:

Received: *21-07-2024*

Revised: *09-09-2024*

Accepted: *29-09-2024*

Abstract:

In today's technological era, the combined problem of assuring user productivity and maintaining strong security standards has become quite a key challenge. As security considerations, have not to hurt productivity, significant efforts must be taken to achieve such goals. The notion of adaptive authentication comes into play to avoid friction in user experience so that a balance between security and user productivity can be maintained. Traditional authentication frameworks are becoming more obsolete due to their ineffectiveness in incorporating additional risk criteria such as location, network type, and operating system into the authentication management process. Adaptive authentication is a combination of authentication and machine learning (ML) technologies that can help in realizing secure intelligent systems. The goal of this research is to provide a complete review of the current applications of various machine learning algorithms often employed in adaptive authentication techniques. Throughout this study, the advantages, limits, and suggestions for future research will be thoroughly discussed.

Keywords: adaptive authentication, machine learning.

I. INTRODUCTION

Adaptive authentication [1] is a mechanism in which the system recognizes risk-related concerns using several environmental and behavioral factors and dynamically customizes the authentication process. This is done by increasing more security layers in case of suspicious behavior. Its purpose is to strike a balance between security and user ease. In a nutshell, adaptive authentication is a method for configuring and deploying two-factor or multi-factor authentication. It is a way for selecting the appropriate authentication elements based on a user's risk profile and scenarios — that is, for adapting the type of authentication according to the situation. There are different ways of deploying Adaptive Authentication procedure; static, dynamic and hybrid but considering the dynamic nature as a challenge, a machine learning-based model could be recognized as an appropriate mechanism for implementation. Machine learning model analyses risk scores based on behavior and context and determines the most effective security response for a certain situation to make the process more salient. The various inputs which are examined for adaptive authentication are environmental factors as geographic location, device-based factors, user-based factors as user age, user role etc. Behavioral factors such as user behavior and geo-velocity are

the most pivotal one to be considered. Then the users are granted access based on risk-score calculated for a series of events. This is where risk-based authentication comes into play. Risk-based authentication is an acronym for adaptive authentication because it is all about determining risks

associated with authentication. Approaches like Adaptive Authentication and machine learning are becoming increasingly necessary in the realm of security, as everything matters in the current day, and it provides a seamless and safe user experience that can keep up with today's continuously growing security breaches. The goal of this research is to provide a detailed review of commonly used machine learning methods.

This research focuses on applying multiple machine learning methods to model user behavior based on contextual information. The following is how the rest of the paper is organized: Section 2 describes the number of existing adaptive systems, Section 3 presents the behavior of authentication Model, Section 4 shows the importance of machine learning in adaptive authentication, Section 5 compares and illustrates the various machine learning Algorithms that can be employed in authentication. Finally, Section 6 discusses the limitations of machine learning in security, and Section 7 concludes.

II. ADAPTIVE SYSTEMS

Not much of the work has been done for machine learning algorithms to be used in adaptive authentication. Some of the adaptive authentication systems have been proposed over the last few years [2][3][4][5]. Researchers have succeeded and implemented a number of existing adaptive systems.

OneLogin

OneLogin adaptive authentication uses machine learning and a wide range of usage patterns pertaining to networks, region, devices and time. The higher the risk level, the greater the diversions from standard usage. Network traffic from a low trust IP address, a black listed country or city, or two places that are far apart will also raise risk scores.

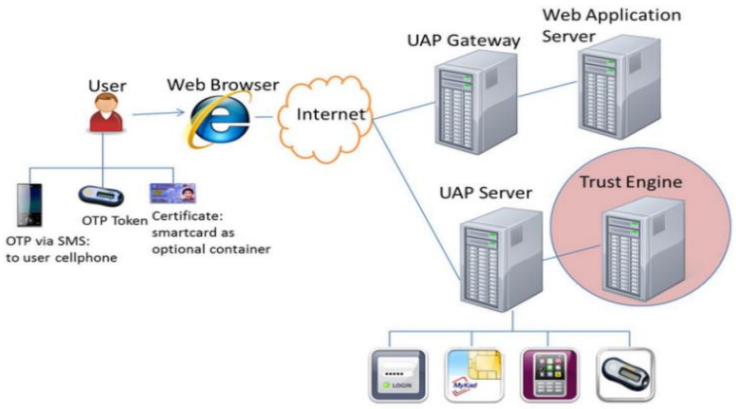
A2BeST

This novel adaptive authentication service is presented by Rocha, Lima and Dantas. This service is based on user's behavior and spatio-temporal context. It detects authentication anomalies using a space-time permutation model and a similarity vector model.

Unified Authentication Platform (*UAP*)

UAP is used to handle user authentication profiles which is a centralized multi-factor authentication system with web based single sign-on (SSO) functionality. Multiple authentication mechanisms are supported by UAP. A variety of applications can re-authenticate itself from different authentication methods using UAP. Figure 1 depicts the general design of UAP.

Figure 1: UAP Design



Learning from user behavior

User behavior can change unpredictably and to overcome this challenging issue, Shi et al proposed an implicit authentication technique that authenticates users based on their behavior. This mechanism gathers and records wealthy data such as location, motion, and communication and application activity.

Secure AUTH

It is to protect sensitive data both internally and externally to our network. It is a push notification when additional factors authentication is required. It generates 4-digit OTP (One Time Password) via SMS or text message or Secure AUTH app. It has the freedom to choose the deployment model that works best on cloud, hybrid, and on-premise.

Centrify

It is for vault access in which factors are decided based on user's context.

WSO2IS

WSO2 identity server is for seamless login experience. It is based on Single Sign-On (SSO), Identity Federation, Authentication - be it multi-factor authentication or adaptive authentication, and more.

The significance of above discussed authentication methods is shown in the tabular form

Table 1: Authentication methods

Adaptive authentication methods	Significance
OneLogin	Secure, Smart, Simple, Scalable
A2BeST	More dynamic, autonomic mechanism
UAP	Single set of login credentials, fewer credentials to remember
Learning user behavior	Increases flexibility, no user input is required
Secure AUTH	Lower cost, customized energy consumption
Centrify	Consistent, easily maintainable
WSO2 IS	Flexible, on-premise & on cloud. Highly extensible, open source

Though learning user behavior relies on machine learning, other methods discussed do not use Machine learning techniques to create the adaptive authentication system.

III. ADAPTIVE AUTHENTICATION MODEL

To model what should be done, there are a set of dimensions to consider as shown in figure 1 and these dimensions can be derived from the answer to basic five questions: Why, When, What, Where and How to adapt ?[6]. An overview of adaption taxonomy for authentication is depicted in figure 2.

Figure 2: Adaptive Authentication Scenarios

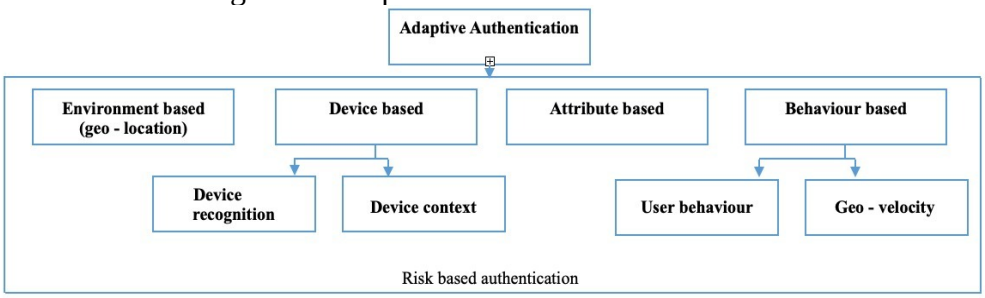
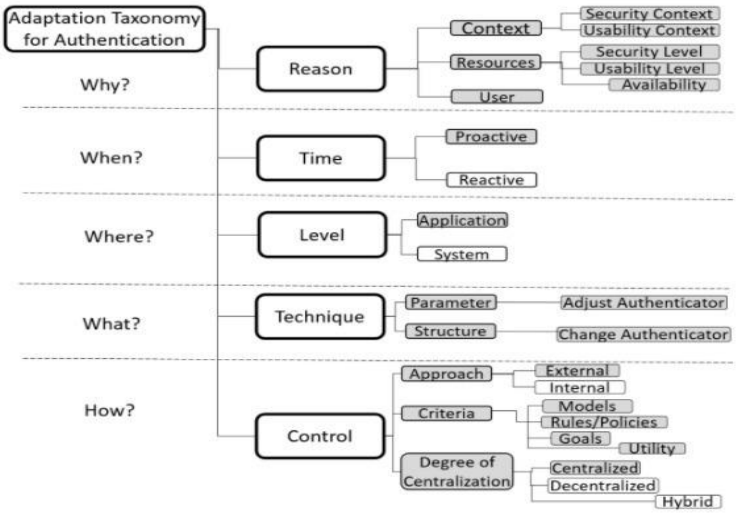


Figure 3: Taxonomy of Adaptive Authentication



•Why to adapt?

As shown in the figure 1. , the adaption reason is due to the change in adaptive systems within three categories namely context (environment), technical resources and user. With regards to context there is a wide range of factors that may impact authentication selection, example: location context, noise levels for voice recognition or battery level. Technical resources are the devices with different authenticators available for the user as face recognition, touch dynamics. Changes on user authentication preferences should be considered for better adaption, example: when a change on the user is detected, adaption is triggered.

•When to adapt?

Reason for this can be reactive or proactive. Reactive adaption is done after an event whereas proactive adaption is done when the adaption logic feels the event that would trigger adaption. Reactive approaches need to monitor user access events whereas a proactive approach continuously monitor and automatically changes the authentication mechanisms when there is a need of more security.

•Where to adapt?

Adaptive authentication can be applied at the system level as well as application level. At system level, selected authenticator gives access to the whole system where as at different authenticators can be selected for different applications.

•What to adapt?

Adaptive authentication adapts both parametric as well as structural technique. In parametric technique relationship between different parameters is used to adjust the system behavior where as structural technique allows changes or addition of components. In authentication domain both techniques are applicable.

•How to adapt?

Adaptive systems consider three different aspects, namely approach, criteria, and degree of centralization. Approach can be either internal which merges the adaption logic with the system resources or it can be external approach which splits the system into the adaption logic and managed

resources. Criteria should be based on rules, policies, goals, combination of different scenarios. The goal should be to choose the best criteria from different possibilities. Adaption logic also considers the degree of centralization which can be centralized, decentralized or hybrid.

IV. MACHINE LEARNING IN ADAPTIVE AUTHENTICATION

Intelligent Adaptive authentication is actually a combination of authentication and Machine Learning algorithms. A branch of Artificial intelligence is Machine Learning which relies on identifying patterns so that authentication can be made to well adapt the situation. Generally additional authentication layer is applied through biometric authentication. Biometric authentication can be physiological as finger print, face recognition and can be behavioral as touch dynamics, mouse movement and gait-based. These factors can be easily implemented through machine learning models which helps the users and devices to continuously authenticate themselves. It helps us to apply authentication in real time.

V. MACNINE LEARNING ALGORITHMS IN AUTNENTICATION

Machine learning models are best suited for this non-static approach because it improves efficiency and accuracy due to its continuous learning behavior, recognizing patterns. It also preserves the notion of usability drives security. In this section, we will discuss different ML algorithms, compare them, and their applications in the security.

The learning algorithms are divided into four classes; supervised, unsupervised, semi-supervised, and reinforcement learning algorithms.

A. Supervised Machine Learning:

This machine learning will make use of the two sets of data — training set and test set. Training set should contain approximately 70% or 80% of data and test set should be 30% or 20%. Training set contains all the inputs and outputs. Supervised learning algorithms represent the relation between the inputs and outputs. Test data are applied on these models to predict their output. Then the accuracy of the model is tested and to improve the accuracy certain parameters are adjusted. Example, if we have events that have been already identified as fraud, then machine learning algorithm determines correlation of features with the result (is the event an fraud or not). Regression algorithms, classification algorithms fall in this category.

B. Unsupervised Machine Learning:

Unsupervised learning does not require labeled data It uses data in which output is not specified..Clustering is an example of unsupervised learning. In clustering similar data items(which are close) falls in one group(cluster) and dissimilar in another. Example if we do not have events that have been already identified as fraud, and then unsupervised learning algorithms can be used. This means, algorithm learns from the data than has not been labeled. These algorithms can’t detect if the authentication is fraud or not, but they can detect anomalies, that potentially could be fraud.

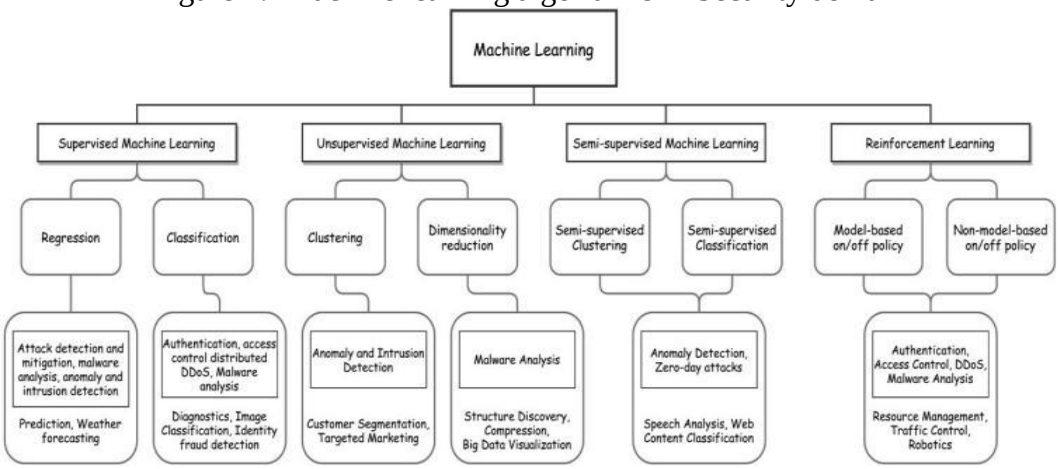
C. Semi-supervised Machine Learning:

Supervised ML makes use of labeled data. Labeled data will take more time to get ready so it increases computational cost, time, and human efforts. Unsupervised ML uses unlabeled data so it is less expensive but its processing is not much accurate. A semi-supervised ML technique is combination of both. It is intended to solve the problem of training huge data for supervised ML algorithms by joining unlabeled data. It seems like semi-supervised ML will perform the best but the accuracy and robustness of semi-supervised ML are still lower than that of supervised ML.

D. Reinforcement Machine Learning (RL):

RL models learn from their own experience, their surroundings and environment. They are used to train themselves. RL model makes use of inputted data only and then the corresponding action is taken depending upon the situation without having prior knowledge. Feedback is given to themselves only to improve its accuracy. An RL technique is of much interest in the authentication domain.The figure 3 shows the various machine algorithms and their applications in the security domain.

Figure 4: Machine learning algorithms in Security domain



Next the analysis of various supervised learning models and unsupervised learning models for adaptive authentication is done.

a) Support Vector Machines (SVM):

The SVMs are supervised models and is a classification technique. The data attributes are divided into two or more classes by a hyper plane in such a way that there is maximum gap between the two classes [7]. The SVMs are notable for their prediction model accuracy while dealing with the visual data [8]. SVMs are mostly used for the dataset with fewer data samples but a large number of data features. SVM is used in security applications to detect network intrusion [9] and spoofing attacks.

b) Bayesian Algorithms:

Bayesian algorithms are based on the Bayes' theorem. It is statistical model that calculates the probability of the event by considering the previous behavior of that event. The most common ML algorithm based on the Bayesian theorem is the Naïve Bayes (NB) algorithm. The NB algorithm is notable for its simplicity. It calculates posterior probability and then uses the Bayesian theorem, to label an unlabeled input. NB algorithm I can be used in network intrusion detection [10].

c) k-Nearest Neighbors (KNN):

KNN is a simplified supervised ML algorithm that can perform both classification and regression. In this algorithm nearest neighbor samples are assigned one class comparing with the unknown data.KNN algorithms are notable for dealing with large datasets. KNN is used to detect network intrusion [11] and malware [12] detection.

d) Artificial Neural Network (ANN):

ANNs are the interconnection of numerous processing elements like the biological neural network of the brain. It consists of an input layer, an output layer, and any number of hidden layers in the network, it creates the classes of input data based on the bias. The researchers of [13] proposed the ANN approach to secure IoT communications.

e) Ensemble Learning (EL):

Ensemble Learning is the most used ML techniques nowadays. EL produces a collective output by combining a lot of classification and regression models to enhance the performance and accuracy of result [14]. Each algorithm in ML has limited accuracy and suitable for specific types of applications and specific datasets. Ensemble Learning takes advantage of all by combining different algorithms together to cover most of the aspects and achieve greater accuracy. Researchers are using Ensemble Learning models to achieve greater accuracy in their models.

f) Principal Component Analysis (PCA)

PCA is a dimensionality (feature) reduction tool which can be applied to a large dataset of different features to reduce them without losing the original information. PCA uses the orthogonality method to make input vectors uncorrelated with each other. It removes the vectors which are rarely needed. It involves the conversion of correlated features into reduced and uncorrelated features [15]. These uncorrelated features are called principal components. Researchers use the PCA technique tin real-time applications for intrusion detection.

g) k-Means Clustering:

K-Means Clustering is the most common approach of unsupervised ML. This technique creates k clusters for data items. The clusters are generally distance-based. The K-means clustering can be used for anomaly detection which can be done by distinguishing between abnormal and normal behavior of data using numbers of similar features. However, the performance of k-means clustering is not so effective as compared to supervised ML models [16]. Generally, the unsupervised ML models are used where the labeling of input data is almost impossible.

The working principle, advantages, disadvantages and applications of above mentioned learning algorithms are represented in tabular form in table 2.and table 3.

Table 2: Machine Learning Algorithms

Models	**Supervised and Unsupervised Learning**		
	Working Principle	**Advantages**	**Disadvantages**
SVM	Generates the classified data by generating a hyperplane in such a way that distance of support vectors with hyperplane is maximum.	Notable for prediction of visual data. Generalization capabilities. Suitable for data with more dimensions but fewer data points.	Difficult to select Kernel version for a specific task. Difficult to comprehend.
NB	Based on Bayes Theorem Posterior probability is calculated to predict possibility of a particular feature set.	Simple Less training data sets are required.	Assumes all features are independent. Zero-frequency problem
KNN	Distance-based algorithm.	Lazy learner Easy to implement	Does not work well with large data set and

	Works on votes for the most frequent label	Can easily identify the intruder attack	high dimensions. Difficult to determine the optimal value of k.
ANN	Attempt to simulate the network of neurons that make a human brain Creates classes of data based on weight and bias.	Can be used to model non-linear and complex relationships Can predict on unseen data	More hidden layers require more processing power. Prediction problems are untraceable
EL	To group weak learners together to form a strong learner	Improves accuracy	Difficult to interpret Increases cost
PCA	Converts the correlated features into reduced number of uncorrelated features(principle components)	Reduces overfitting Improves visualization	Information loss may happen Needs another ML technique to work with
K-Means	Makes clusters on feature similarity	Can easily detect intrusion because of separate clusters.	Not suitable to identify clusters with non-convex shapes.

Table 3: Machine Learning Algorithms Applications

Models	**Applications in Security**
SVM	Detection of malware attacks in a smart environment. Network intrusion detection
NB	Intrusion detection in networks
KNN	Intrusion detection and anomaly detection
ANN	Detection of various classified attacks with greater accuracy
EL	Enhanced detection of intrusion, anomaly, malware
PCA	Real-time detection systems in IoT networks.
K-Means	Distinguish between normal and abnormal networks.

Biometric authentication which performs the verification by checking distinctive biological or behavioral characteristics is generally applied as an additional security layer. As touch dynamics is one of the important behavioral biometrics authenticator, the analysis of it using different classifiers by different researchers is presented here.

Touch dynamics biometrics refers to the process of measuring and assessing human touch rhythm on touch screen devices (e.g. smart phones). A form of digital signatures is generated upon human

interactions with these devices. These signatures are discriminator and unique for each individual, so may be used as a personal identifier.

Touch dynamics authentication system can be deployed in one of the two modes verification mode and identification mode. These modes serve different purposes and usage scenarios. The verification mode is used to verify a claimed identity. It is used to answer the question “is this person whom he/she claims to be”. Example, authentication of a mobile user. The identification mode, on the other hand, is used to classify and identify some unknown identity. It is used to answer questions such as “who is this person” or “is this person in the database. Here the analysis is on the verification mode. To assess the suitability of a biometrics authentication method to real-world applications, major criteria to evaluate the system is verification accuracy.

The metrics that are commonly used to evaluate the verification accuracy of a biometrics authentication method are the False Rejection Rate (FRR), False Acceptance Rate (FAR) and Equal Error Rate (EER). False Rejection Rate (FRR) is the percentage ratio of the number of legitimate users who are falsely rejected against the total number of legitimate user trials. Other terms used for FRR are false alarm rate, false negative rate, false non-match rate, or Type II error. False Acceptance Rate (FAR) is the percentage ratio of the number of illegitimate users who are falsely accepted against the total number of illegitimate user trials. Lower FAR value will indicate that the system has a higher security level. FAR is also referred to as miss alarm rate, false positive rate, false match rate, or Type I error. Equal Error Rate (EER): EER is a single-number performance metric, which is commonly used to measure and compare the overall accuracy level of different biometrics authentication method. It is also known as Crossover Error Rate (CER). In real- life applications, FRR and FAR are usually adjusted and determined based on the security and usability requirements of the applications. The term ‘accuracy’, can also be used for EER, which is an accuracy performance metric.

Review of different researchers :

Feng et.al[19] proposed FAST, a touch based user authentication mechanism, they then constructed 53 features for each touch gesture. In the user study with a total of 40 participants, they achieved a False Accept Rate (FAR) of 4.66 % and False Reject Rate of 0.13 % in the login phase.

In the same year, Meng et al. [20] presented the concept of touch dynamics and particularly extracted 21 different features using SVM classifier.In the study, they have 20 participants and designed a hybrid classifier called PSORBFN. With this classifier, they could achieve an average error rate of 2.92 % (FAR of 2.5 % and FRR of 3.34 %).

Frank et al. [17] designed a proof-of-concept classification framework to collect a set of 30 behavioral features that can be extracted from the touch screen input using a nearest neighbor classifier and a Gaussian RBF kernel support vector machine (SVM). These classifiers could achieve robust authentication results, with equal error rates (EERs) between 0 and 4 %, depending on the application scenario.

Li et al. [18] presented a re-authentication system based on users’ finger movements. In particular, they used 13 metrics to measure a sliding gesture such as first touch position, first touch pressure, first touch area, and first moving direction. . They then conducted a study with 75 users. With SVM classifier, they could achieve the best accuracy of 95.78 % for sliding up gestures.

Meng et al. [21, 22] then identified that the selection of classifiers may impact the authentication performance, so they designed an adaptive mechanism that can periodically select a better classifier to maintain the authentication accuracy during user authentication. They evaluated with 50 participants, the experimental results demonstrated that the adaptive authentication scheme can

achieve an average error rate of 2.46 %.

Meng et al. [23] further took the authentication system to a good level by developing a touch movement- based security mechanism, called TMGuard, to enhance the authentication security by evaluating 75 participants. They found that taking 9-dot patterns as an example, the successful rate is decreased from 97.8 % to 91.1 % for males and from 97.8 % to 88.9 % for females, respectively.

A summary of touch dynamics-based user authentication schemes is represented in the tabular form in table 4.

Table 4: Touch Dynamics-based User Authentication Schemes

Study	Classifiers	No.of users	Mechanism with features	Performance
Feng et al. [19] in 2012	Random forest, Bayes Net	40	FAST with 53 features	FAR: 4.66 % FRR: 0.13 %
Meng et al. [20] in 2012	SVM	20	A touch dynamics-based authentication scheme with 21 features	FAR: 2.5 % FRR: 3.34 %
Frank et al. [17] in 2013	SVM	41	Touchalytics with 30 features	ERR: nearly 4 %
Li et al. [18] in 20 13	SVM	75	Sliding gesture with 13features	Best Acc.: 95.78 % for sliding up
Meng et al. [21] in 2014		50	Adaptive authentication scheme with eight features	FAR: 2.55 % FRR: 2.37 %
Meng et al. [23] in 2016		75	TMGuard	EER: 1–3 %

VI. LIMITATIONS OF MACHINE LEARNING IN SECURITY

In ML training, accurate results can be achieved when training is performed with a bulk of initial dataset before subjecting the algorithm for classification purposes. There is a bulk of data available from various types of devices; the security-related data is not available in a sufficient amount. Moreover, there is an issue in using some confidential data for every algorithm to train. So, there is a need to develop a crowd-sourcing platform to create different datasets for different security tasks. These datasets should include all authentication types and attack patterns so that the ML algorithms can be easily trained. This will also help to set the standards of classifiers by testing them on that dataset. There should also continuously monitor and patterns for new attacks that should be added in datasets. As data is collected from heterogeneous devices, data is not cleaned. This low-level data can be noisy data or corrupted data which can affect the ML model while training. So, there should be filtration of data that can be sent to the ML model to train in real-time.

VII. CONCLUSION

Most risk-based authentication solutions use machine learning. In adaptive authentication, one has to regulate the parameter weight for the risk score by introducing static policies according to factors gathered from the user. These algorithms help to monitor in real time and to identify anomalies in

user's authentication pattern or even threats in the authentication path (such as compromised networks). This paper presented an overview of adaptive authentication using machine learning algorithms which included behavioral, physiological methods. We have tried to focus on comparing different supervised and unsupervised learning methods on their applications in authentication, advantages, disadvantages. We have also compiled the basics information about types of learning like supervised, unsupervised, and reinforcement learning and provide a short insight of them. We also have shed light on the limitations of using ML in security. Different authentication methods are discussed but more work can be done on it and authentication schemes can be re-designed to be lightweight, collaborative and flexible. To fulfill the critical requirements for security, hybrid approach instead of either centralized or only distributed approach can be used along with ML for authentication.

VIII. References

[1] K. A. A. Bakar and G. R. Haron, "Adaptive authentication: Issues and challenges," 2013 World Congress on Computer and Information Technology (WCCIT), 2013, pp. 1-6.

[2] C. Rocha, J. C. D. Lima, M. A. R. Dantas and I. Augustin, "A2BeST: An adaptive authentication service based on mobile user's behavior and spatio-temporal context," 2011 IEEE Symposium on Computers and Communications (ISCC), 2011, pp. 771-774.

[3] A. Moss, S. Liu and R. Richard, "A Unified Authentication Framework for Accessing Heterogeneous Web Services," 2008 4th International Conference on Next Generation Web Services Practices, 2008, pp. 117-122.

[4] Abu Bakar, Khairul Azmi, Haron, Galoh "Adaptive authentication based on analysis of user behavior", Proceedings of 2014 Science and Information Conference, 2014.

[5] Elaine Shi, Yuan Niu, Markus Jakobsson, Richard Chow "Implicit Authentication through Learning User Behavior" in Proceedings of the 13th International Conference on Information Security, 2011, pp. 99–113.

[6] C. Krupitzer, F. M. Roth, S. VanSyckel, G. Schiele, and C. Becker. A survey on engineering approaches for self-adaptive systems. Pervasive and Mobile Computing, 17:184–206, 2015.

[7] S. Tong and D. Koller, Support vector machine active learning with applications to text classification, Journal of machine learning research, vol. 2, no. Nov, pp. 45-66, 2001.

[8] A. Qureshi, K. B. Khan, H. A. Haider, R Ensemble Classification-Based Methodology Applied to MRI Brain Technologies and Applications (INTAP), pp 606-615, 2020.

[9] M. Abu Alsheikh, S. Lin, D. Niyato, and H. P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," IEEE Commun. Surveys and Tutorials, vol. 16, no. 4, pp. 1996–2018, Apr. 2014.

[10] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "A system for Denial-of-Service attack detection based on multivariate correlation analysis," IEEE Trans. Parallel and Distributed Systems, vol. 25, no. 2, pp. 447–456, May 2013.

[11] J.W. Branch, C. Giannella, B. Szymanski, R. Wolff, and H. Kargupta, "In-network outlier detection in wireless sensor networks," Knowledge and Information Systems, vol. 34, no. 1, pp. 23–54, Jan. 2013.

[12] F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, "Evaluation of machine learning classifiers for mobile malware detection," Soft Computing, vol. 20, no. 1, pp. 343–357, Jan. 2016.

[13] M. A. Aref, S. K. Jayaweera, and S. Machuzak, "Multi-agent reinforcement learning based cognitive anti-jamming," in Proc. IEEE Wireless Commun. and Networking Conf (WCNC), pp. 1–6, San Francisco, CA, Mar. 2017.

[14] Wozniak, Michal Graña, Corchado Emilio "A survey of multiple classifier systems as hybrid systems", Information Fusion, vol. 16, pp. 3-17, 2014.

[15] G. Han, L. Xiao, and H. V. Poor, "Two-dimensional anti-jamming communication based on deep reinforcement learning," in IEEE Int'l Conf. Acoustics, Speech and Signal Processing, pp. 2087–2091, New Orleans, LA, Mar. 2017.

[16] C. Shi, J. Liu, H. Liu, and Y. Chen, "Smart user authentication through actuation of daily activities leveraging WiFi-enabled IoT," in Proc. ACM Int Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 1–10, Chennai, India, Jul. 2017.

[17] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touch analytic: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 136–148, Jan 2013.

[18] L. Li, X. Zhao, and G. Xue, "Unobservable reauthentication for smart phones," in Proceedings of the 20th Network and Distributed System Security Symposium, 2014.

[19] T. Feng, Z. Liu, K.-A. Kwon, W. Shi, B. Carbunar, Y. Jiang, and N. Nguyen, "Continuous mobile authentication using touchscreen gestures," in IEEE Conference on Technologies for Homeland Security, Nov 2012, pp. 451–456.

[20] Y. Meng, D.S. Wong, R. Schlegel, L.-F. Kwok, Touch gestures based biometric authentication scheme for

touchscreen mobile phones, in Proceedings of the 8th China International Conference on Information Security and Cryptology (INSCRYPT). Lecture Notes in Computer Science, vol. 7763 (Springer, 2012), pp. 331–350, Beijing
[21] Y. Meng, D.S. Wong, L.F. Kwok, Design of touch dynamics based user authentication with an adaptive mechanism on mobile phones, in Proceedings of the 29th Annual ACM Symposium on Applied Computing (ACM SAC), Gyeongju (2014), pp. 1680–1687
[22] W. Meng, D.S. Wong, L.F. Kwok, The effect of adaptive mechanism on behavioural biometric based mobile phone authentication. Inf. Manage. Comput. Secur. 22(2), 155–166 (2014)
[23] W. Meng, W. Li, D.S. Wong, J. Zhou, TMGuard: a touch movement-based security mechanism for screen unlock patterns on smartphones, in Proceedings of the 14th International Conference on Applied Cryptography and Network Security (ACNS 2016), Guildford (2016), pp. 629–647
[24] V. M. Patel, R. Chellappa, D. Chandra and B. Barbello, "Continuous User Authentication on Mobile Devices: Recent progress and remaining challenges," in IEEE Signal Processing Magazine, vol. 33, no. 4, pp. 49-61, July 2016
[25] T. Neal, D. Woodard, and A. Striegel, “Mobile device application, bluetooth, and wi-fi usage data as behavioral biometric traits,” in IEEE International Conference on Biometrics Theory, Applications and Systems, Sept 2015, pp. 1–6.
[26] https://www.chakray.com/what-is-adaptive-authentication-and-what-are-its-challenges/