RISK-BASED AUTHENTICATION FOR ONLINE FINANCIAL SERVICES

Ajay Benadict Antony Raju
ajaybenadict@gmail.com

Abstract

Risk-Based Authentication (RBA) can be described as a sophisticated security model that adapts an authentication process depending upon the risk evaluation of a user login. Unlike RBA, standard authentication factors are set and permanent, for example, passwords or PIN numbers, while others are dynamic taking into consideration such things as device type, IP address, geographical location and previous activity of the user. This dynamic mechanism makes online financial services capable of offering better security without turning the user interface into a fortress by applying only complex and higher authentication factors when the utmost security is required.

As for the role of security in the further development of online financial services and banking and investment platforms, it is safe to state that it has been never so important as it is now due to the exponential growth of digital services. Because RBA can dynamically add or remove protections and update protection settings to counter new risks and users' new behaviors, it is crucial for today's financial cyber defense solutions. That is why RBA systems have the potential to reverse-engineer the risk assessment process with the help of artificial intelligence (AI) and machine learning (ML), which enables constant learning and enhancing of the risk assessment algorithms that identify anomalies and fraud.

Nevertheless, when it comes the actual implementation of RBA, it is by all means no problem free. Aspects like security of users and objects, false positive ratio, and the most important fairness and explain ability of artificial intelligence decisions are concerned. This paper aims at examining the working of RBA, its advantages and disadvantage, and the kind of security it brought for protecting the emerging territory of internet based financial services. Moreover, this paper presents literature research on RBA, a comparison of the existing frameworks, an evaluation of this study's framework's deficiencies, the proposal of an improved RBA model, which would lead to the creation of a more secure and user-friendly approach to financial transactions.

Keywords: Risk-Based Authentication, Online Financial Services, Adaptive Security, Machine Learning, Fraud Prevention, User Experience

I. INTRODUCTION

It should be noted that nowadays the financial services industry has been actively developing due to the use of new technologies. This is because consumers are today opting for online financial services such as banking and payment, investment and insurance among others due to reasons such as convenience. While accepting this new trend as inevitable and beneficial on the whole, there are also new and manifold security risks that stem from this process. Hacker continues to be active in their modality leveraging on phishing, social engineering, malware and credential stuffing to infiltrate online services. Thus, the protection of the financial transactions performed over the Internet is one of the critical and major concerns of the financial institutions, governments and regulations agencies.

Standard forms of identification that include passwords, Personal Identification Numbers and security questions have been found to be incapable of tackling these threats. This makes these methods static and susceptible to a broad range of penetration testing techniques such as phishing, brute force as well as credential reuse. Once such details are in the wrong hands, they can be used to fraudulently access individuals' confidential financial accounts with severe repercussions for monetary losses, and the tarnishing of the image of the consumers and the financial institutions in question. Furthermore, more effective methods such as, Multi-factor Authentication help in developing a barrier to unauthorized access, but they also tend to be inconvenient and complex when implemented, hence lowering usage and UX. Protecting assets and customers' data while ensuring that the vice is easily accessible has thus been a major consideration to the financial services industry.

Due to these increasing concerns, the Risk-Based Authentication (RBA) has been developed as a more effective general framework for protecting the online financial services. Namely, RBA analyses several contextual and behavioural features to determine the risk level of each login attempt or transaction. Due to the analysis of device details, IP address, geographic location and behaviour, the RBA system can decide whether a connection is genuine or probably an attempt at intrusion. The low-risk activities can continue with minimal interference while high risk activities caused increased security measures including two factor authentication process, known-test questions or user account lockouts.

The rather promising concept behind RBA is the flexibility of the model. RBA is clearly more beneficial than static methods because it adapts the security requirements in real time depending on the evaluation of the risk. This is done to allow all users including the legal one's ease of access to their account without much problem, while the suspicious activities are either denied or questioned. In addition, RBA systems that incorporate AI and ML enable longer learning periods, thus enabling the system to arrive at improved risk judgments while eliminating many false negative and positive outcomes.

Because of even higher complexity and scalability of today's cyber threats RBA is finding its way as one of the indispensable elements of financial security systems in the era of web-based services. However, its implementation presents some issues which need to be solved: there is no transparent AI-decision-making in current systems; disruption of users is not always minimized; there is no integration between various RBA systems. This paper aims at analysing the current status of RBA in online financial services, the advantages & disadvantages as well as its future prospect in providing high end solution to the fight against financial cyber-crime.

II. LITERATURE REVIEW

The advancement of Fin Tech has led to a rise in the study of new security systems with RBA as an example of adaptive solutions. Initial research has highlighted the fact that the use of passwords and static tokens has a major drawback that forms the basis of many extreme cyber criminology attacks that makes it necessary to use dynamic solutions. Still, due to RBA's capability to evaluate contextual data such as the device's fingerprint, IP address, and geolocation, it is considered a rather suitable option 【2】.

A number of scholars have also investigated how AI and ML can be applied in RBA systems Many scholars have also studied how the application of AI and Machine learning could be incorporated in RBA systems. These technologies complement RBA's capacity to identify deviations and estimate probable cyber threats on the network in real-time【3】. It was reported that with the deployment of AI in RBA, there are far fewer false positives and the user will only be prompted on potentially high-risk transactions【4】. However, by leveraging AI, there are issues to do with transparency and algorithmic premised equity, which must be worked to observing fairness】.

However, present day RBA frameworks come with some limitations as discussed in this paper. Currently, there are systems that can work perfectly with other security models, but not with other protocols【6】. Also, RBA faces the issue of having no set methods, which would give an understanding of the risk level of logins, which causes distortions in its implementation. Hence, it becomes imperative to continue the study to create more effective, more flexible, and more transparent RBA models that should be universally applicable on the financial level.

III. PROBLEM STATEMENT

Although Risk Based Authentication (RBA) has a potential solution for increasing the level of security for the online financial services, there some barriers that can hamper with the efficiency of implementation of the RBA. Some of today's advanced RBA solutions have the problem of maintaining an appropriate level of security when implementing the convenience for users. Those cases can produce high false positive rates which may cause user frustration and abandoned transactions or false negative rates that may lead to unnoticed security vulnerabilities【2】【3】. Further, there is no uniformity in terms of RBA frameworks and, hence, the metrics for integration with the varied sorts of financial platforms【1】. Furthermore, there are some issues that arise with the AI-based RBA systems that are: The issues of opacity of algorithms, and the issue of fairness. Thus, to address these issues, there is a necessity to improve and optimise RBA systems to make them reliable and easy to use in online context of financial services.

IV. SOLUTION

Due to possible obsolesces and complications of current RBA systems, dynamic and integrated approach is required to accommodate all of them. Today's proposed approach adds machine learning, multi-stockpile verification, XAI, ISO metrics, and perpetual supervision to optimise effectiveness, luminosity, and non-biased utilisation of RBA for online money services.

At the heart of the solution that we are proposing is the use of better machine learning algorithms that are much more complex. Legacy RBA systems are usually based on a set of rules and fixed thresholds which may not be sufficient to address new threats and new user behaviour. Confronting the problem of Fraudster ry and Account Compromise Through RBA systems with the help of advanced Machine learning such as deep learning and Ensemble method, RBA system can identify more significant contextual information and can identify more significant patterns that indicate Fraud or account compromise in the future (Liu, Steffen, & Rubin, 2019) 【3】. These algorithms learn iteratively and the ability of deciding levels of risk also improve with time. Dynamic learning enhances the possibility of the system and the increase in new forms of threats or the change in users' behaviour which will in turn decrease both false positive and false negatives (Ni, Li, & Feng, 2020) 【4】.

The other important part of the solution is a multiple layer verification system. This approach divides the attempted logins into three different risk categories which are low, medium, and high then responds with appropriate safeguards depending on the evaluated risk level (Frey & Rückes, 2019) 【2】. Normal risk logins have few events of identification with the users getting to log in easily. Medium risk logins may require extra check, for instance questions or device confirmation and high-risk logins may require more MFA security feature (Liu et al., 2019) 【3】. This approach suit user convenience best by only minimally investigating legitimate users while scrutinizing potentially risky activities more.

Due to some criticisms that are related to algorithm selection and the fairness of the particular algorithms, the solution includes xAIES techniques. Explana AwAI in the system enables users and administrators to comprehend the rationale behind specific security determinations hence enhancing fairness of the decisions made (O'Neil, 2016) 【5】. Ensuring that the reasons behind the certain security measures are explicated, explainable AI assists users in accepting the actions taken by the system and enables administrators to supervise and analyse the system to eliminate biases and mistakes (Ni et al., 2020) 【5】.

To use the words of Ates, et al. (2013), the proposed method also includes the vital standardisation of goals as well as guidelines. There is still uncertainty and variability regarding the general structure of RBA frameworks and the measures used for evaluating their efficiency, which often makes integration of RBA systems across the different platforms problematic (Bonneau, Herley, van Oorschot, & Stajano, 2012) 【1】. It will include identifying and developing regular benchmarks to work against when giving structure and algorithm to RBA, relating best practices for its application with other layers of security, and most importantly ensure compatibility with different forms of finance. This type of approach will ensure that more organisations implement RBA systems and that the implemented systems operate in a standardized manner.

Last but not the least; constant vigil and periodically making changes are crucial to sustenance of Right-Based Approach or RBA systems. Continuous monitoring requires the analysis of users' actions and interactions with systems in real time to potential signs of malicious behaviour and adapt risk levels, if necessary (Frey & Rückes, 2019) [2]. The use of real-time analytics and feedback loops enables RBA system to be continually relevant against new emerging threats.

Altogether, the proposed solution can be considered as an improvement of Risk-Based Authentication as it includes the usage of modern machine learning algorithms, the multi-step verification process, the usage of xAI, the unity in metrics and guidelines, and constant monitoring and improvement. This wide-ranging strategy takes on the major issues that contemporary RBA systems face and offers a sound model for hacking safe online payments and effective, friendly client satisfaction.

V. CONCLUSION

It implies that Risk-Based Authentication (RBA) is the next step in protecting online financial services from the deficiencies of static identification methods that are easy to crack by today's cyber threats. Flexible where the security requirement changes according to risk level of the login attempts, RBA is a security solution that adds to the security of the system and the usability. With more and more financial services shifting toward online-based formats, the need for enhanced solution like RBA rises significantly. But the application of RBA has not been smooth in the automotive industry, it has had some problems.

There are still some problems with these implementations, at least two, which is the security and the usability. This is true since most users would get frustrated once they are repeatedly responding to what the system has deemed as threats when in the real sense; they were not actually a threat and will thus abandon certain transactions. At the same time, such systems may not be capable of identifying threats, that in reality were otherwise impending and this makes the system vulnerable to attacks. Moreover, there is a lack of consistency in the application of RBA due to variations in RBA frameworks and metrics used by various advisory firms, and thus leading to a reduced efficacy of this advisory model when adopted across the various leading financial platforms. Moreover, with the help of advanced technologies, such as artificial intelligence and machine learning, the RBA's capability to identify and prevent fraud in real-time has been improved; however, the issues related to the interpretability and fairness of these algorithms have to be solved in order to gain users' trust and employ them responsibly.

In order to meet these concerns, a new RBA model with improved algorithms of Machine learning is mandatory along with multiple safeguards. By developing such a system, false positive and false negative results can be minimised due to more accurate identification of typical and anomalous behaviour. In addition, for improvement of explain ability and addressing the problem of algorithmic bias, the use of XAI techniques should be incorporated. Standard rules or benchmarks for the application of RBA into the various sectors particularly the financial service providers would also help in standardizing and broadening the usage of the concept.

Therefore, Risk-Based Authentication may be seen as a way how to advance the security of online financial services. This way, the financial industry will be protected from risks while making RBA systems more user-friendly since the problems existing in this sphere are recognized and worked on constantly. Today, the digital world is constantly changing and it is the same with solutions that help protect personal data, and RBA is one of the leaders in such developments. Further research and developments in this field will however be very important in that they will help to ensure RBA continue to acts as a sound security model in an ever-complex security environment.

REFERENCES

1. Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. Proceedings of the IEEE Symposium on Security and Privacy (SP), 553–567. https://doi.org/10.1109/SP.2012.44
2. Frey, S., & Rückes, S. (2019). Risk-based authentication: Tracking, detection, and attack prevention in user sessions. Information Systems Security, 28(4), 188–202.

https://doi.org/10.1080/1065898X.2019.1632223

3. Liu, Y., Steffen, M., & Rubin, A. D. (2019). Learning-based risk-aware authentication. Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security (AsiaCCS), 277–290. https://doi.org/10.1145/3321705.3329840
4. Ni, Z., Li, Y., & Feng, D. (2020). Towards an AI-powered adaptive authentication system: A survey. IEEE Access, 8, 83713–83734. https://doi.org/10.1109/ACCESS.2020.2991667
5. O'Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. Crown Publishing Group.