Authentication Technique Based on Image Recognition: Example of Quantitative Evaluation by Probabilistic Model Checker

Bojan Nokovic

McMaster University, Computing and Software Department,
1280 Main Street West, Hamilton, Ontario, Canada

Abstract. A probabilistic model checker is a software tool for formal modeling and analysis of systems that exhibit random or probabilistic behaviour. Over probabilistic models, we analyze an innovative online authentication process based on image recognition. For true positive identification, the user needs to recognize the relationship between identified objects on distinct images which we call an outer relation, and the relation between objects in the same image which we call an inner relation. We use probabilistic computational tree logic formulas (PCTL) to quantify false-negative detection and analyze the proposed authentication process. That helps to tune up the process and make it more convenient for the user while maintaining the integrity of the authentication process.

Key words: Hierarchical State Machines; Probabilistic Model Checker; Costs/rewards; Verification

1 Introduction

Software applications called web robots or *bots* create the majority of web traffic [6]. We can divide bots to *good* bots, and *bad* bots. Good bots are used for website health checks, to extract authorized data, to collect data for search engine algorithms, etc. Bad bots are used to bypass security using a false identity, extract unauthorized data, and inject spam links, malware, etc. Bad bots that present false identities to bypass security are called *impersonators* and create 84% of all bad bot web traffic. In this work, we analyze the impact of impersonators on an advanced image-based authentication technique patented by Royal Bank Canada (RBC). The patent is designed to provide protection from impersonators. The goal of our work is to increase the confidence that the user or subject is who he claims to be. Our process of a user's identity recognition has two levels. On the first level, based on the system information like keystroke dynamics, mouse movement, location (etc.) we estimate the probability of bot presence. If we detect the bot at this level, the authentication is complete. If the bot is not detected the second level of the authentication process is performed that consists of questions related to

1. image context
2. the semantics of presented images
3. outer and inner relations between images are presented

David C. Wyld et al. (Eds): SOEN, SIPP, PDTCA, ITE, CCSIT, NLPCL, DaKM, BIGML, AISC -2023
pp. 69-84, 2023. CS & IT - CSCP 2023 DOI: 10.5121/csit.2023.131206

Based on the answer to these questions, we can increase confidence in our decision. An integral part of the patent is ML which helps in understanding and responding to a variety of bot behaviours. The system is capable of improving itself. This is especially important knowing that bad bots are *improving* their bad skills too.

While patents are registered innovative ideas, building a successful product around the patent requires fine-tuning of patent components. That is usually done by testing a prototype, but building a prototype requires a significant amount of time and resources. In this paper, we explore the notion of using modelling in the authentication domain. To reduce the time to build a market-ready system, we build a model of the proposed system. Instead of building a prototype, a model of the patent is built where we can estimate its effectiveness and tune various parameters.

In section 2 we look at other authentication processes and show that our approach is an evolutionary step further compared to existing systems. Next in section 3 we provide a mathematical model of an authentication system based on set theory. In section 4 we provide a probabilistic model of subject behaviour and estimate authentication confidence as a probability of true positive detection. In section 5 we discuss how ML can further increase confidence in an authentication process and present the *rate* of false positive and false negative detection. The work is wrapped with the conclusion of the current work and its possible extension.

2 Related Work

Bots mimic human behavior and may not be detected by traditional security tools. Because of that in the last decade number of special bot detection algorithms mostly based on traffic behavior and analysis are proposed [16] [17] [9]. Experimental results suggest that those methods are effective and robust. It is shown that bots or computers can be detected successfully using ML models [4]. Using the collected information, ML tools report on fraudulent attempts. Continuous improvement of a data model is embedded into systems. However, ML in this context relies on employing engineered features such as *friend-to-followers ratio* on social media platforms (SMPs) [15] or on people reporting discrepancies in their credit card activity. In applying ML to user authentication, the focus of the model shifts from fraud detection to identity assurance [11]. It is shown that by learning from data in users' past authentication attempts, such as location/network, time of day, device fingerprint, pattern of access, and keystroke dynamics we can increase the confidence that a given user is who he or she claims to be. Our work is the continuation of this approach. Image recognition can further strengthen our confidence in the authentication process. In ML data sets, the pattern of image recognition challenge is added. If the system is confident that a bot is identified with some probability greater than threshold, a more challenging image recognition problem is presented.

The procedure that requires online banking customers to provide personal verification questions (PVQ) is standard practice in many financial institutions [1]. Customers are asked to provide three to five PVQs that are used to issue a new password in the event customer forgets the original password. Our system of web robot detection is fully compatible with PVQ. The intention is not to replace PVQ, but to add a new layer of verification.

Software systems are traditionally constructed *deductively* by program code as the rules that govern the system behaviors, but with ML techniques those rules can be changed *inductively* from a set of trained data [7].

MFA based on face recognition and image recognition may significantly reduce the risk of identity compromise over passwords [14], but none of those techniques are based on the relations between images. To the best of our knowledge, our system is the first that requires the detection of both *outer* relations between images and *inner* relations inside images during an authentication process.

3 Authentication Process

Our system is designed in a way that makes the authentication process different for a bot, but easy for a human. Authentication is the process in which the subject, which may be human or bot, should demonstrate some form of evidence to prove its identity. Two sets of images are presented to the subject, one set contains a visual question, and another set contains a solution. The question set, we call it A, contains n images $A = \{a_0, a_1, .., a_n\}$ that has some kind of relation. In addition to the relation between images, there may also be the relation between objects inside a single image. Another set of images, $B = \{b_0, b_1, .., b_n\}$, has one image that should logically be in the same type of relation to the subject, as the relation between pictures inside set A. The authentication process requires finding out the image from set B that has the same relation to the subject as

1. relation between images, form set A
2. relation between objects inside some of the images from set A.

Let $\mathscr{R}$ be *a relation on a set* A or a relation from A to A. In other words, a relation on a set A is a subset of $A \times A$. Let A be the set $\{Dog, Cat, Mouse\}$. Order pairs that satisfies the relation $\mathscr{R} = \{(a,b) | a \text{ "eats" } b\}$ are

$$\mathscr{R} = \{(Dog, Cat), (Cat, Mouse)\}$$

The relation *eats* indicates that a dog is a natural predator of a cat and a cat is a natural predator of a mouse. The relation $\mathscr{R}$ on the set A is

- *irreflexive*, $(Dog, Dog) \notin \mathscr{R}$
- *antisymmetric*, $(Dog, Cat) \in \mathscr{R} \Rightarrow (Cat, Dog) \notin \mathscr{R}$
- *intransitive*, $(Dog, Cat) \in \mathscr{R} \wedge (Cat, Mouse) \in \mathscr{R} \Rightarrow (Dog, Mouse) \notin \mathscr{R}$

Let B be the set $\{Lion, Alligator, Hamburger\}$, and C be the set of one abstract element authentication subject $\{Subject\}$. A *binary relation* from C to B is a subset of

$$C \times B = \{(Subject, Lion), (Subject, Alligator), (Subject, Hamburger)\}$$

The only subset that satisfies relation $\mathscr{R}$ is

$$\mathscr{R} = \{(Subject, Hamburger)\}$$

Meaning that only *Hamburger* is the correct answer. This solution is intuitive for the subject human, but for the bot, it is not. To solve this visual question a bot needs to (1) recognize objects on each image and (2) find a semantical relation between objects presented on images. To make that process even more difficult for the bot, we allow the presentation of multiple objects on the same image. In addition to the relation between images, the bot needs to find out the relation between identified objects inside the same picture.

Example Consider the authentication process shown in Figure 1. Set A is the set that contains $\{Cat, Mouse, \{Mom, Baby\}\}$.
Order pair that satisfies the relation $\mathscr{R} = \{(a,b)|a \text{ "eats" } b\}$ is

$$\mathscr{R} = \{(Cat, Mouse)\}$$

The third element of set A is the set of two elements $\{Mom, Baby\}$. *Visual* relation between those elements can be described as $\mathscr{R}_v = \{(a,b)|a \text{ "feeds" } b\}$. Again the only subset of binary relation $C \times B$ is $(Subject, Hamburger)$, and

$$\mathscr{R} = \{(Subject, Hamburger)\}$$
$$\mathscr{R}_v = \{(Subject, Hamburger)\}$$

To successfully find out the right element form set B, the *Subject* needs to

- Find the relation $\mathscr{R}$. Recognize pictures and find out the set of possible relations between those pictures. Each picture can be described as *noun*. There may be multiple, but finite number of relations $\mathscr{R}_1, \mathscr{R}_2 .. \mathscr{R}_n$ between images.
- Find out the relation $\mathscr{R}_v$. This is the relation between *subjects* on the same picture. The relation shown on the picture has to be clear and to have clear meaning. The relation is a *verb*, and set of relations should contain only one element.
- Find $\mathscr{R}_i$, i $\in (1..n)$ that has the strongest semantic similarity to $\mathscr{R}_v$
- Select the picture *Solution* from the set B such that

$$\mathscr{R}_i = \{(Subject, Solution)\}$$
$$\mathscr{R}_v = \{(Subject, Solution)\}$$

Although advanced bots are capable to analyze syntax and even the semantics of an image to some extent, it is hard for bots to figure out the relation between presented images. The authentication process has two major components: image recognition, and the subject discovery process performed by a computerized system. In our model, for those two major components, we assume

- The subject human is always more *skillful* than the subject bot, meaning the human is more likely to discover the relation between images and especially inside images than a bot.
- User interface components, user agent, and machine or device *signature* can recognize bot 80% of the time. The system presented in [3] that employs behavioral biometrics, including mouse and keystroke dynamics, is capable to detect 97.9% of *blog bots* with a false positive rate of 0.2%. In our conservative estimation, we assume that our system can positively distinguish a bot from a human 80% of the time.

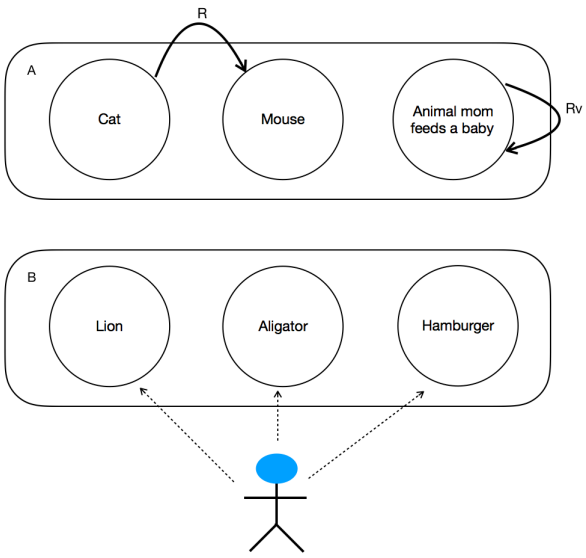

Fig. 1. Authentication

Inevitably it will happen that (1) the bot selects the correct image (2) the human selects the incorrect image. In the first case, when the bot selects the correct image without additional verification, the bot may be granted access to unauthorized data. In the second case, the user will not have access to his own data. Those four combinations and their impact on the system are shown in Table 1.

Table 1. Authentication options

Image	Human	Bot	Impact	Damage
Correct	Yes	No	No	No
Correct	No	Yes	Yes	Severe
Incorrect	Yes	No	Yes	Low
Incorrect	No	Yes	No	No

The system must be designed in a such way that the probability of severe damage caused by the bot during the lifetime of the system is extremely low, close to zero. At the same time, we wish to minimize the damage caused by the failure to authenticate the right user.

We divided human authentication subjects into three σ groups based on image recognition skills. We follow a normal distribution, average customers of level $\sigma 1$ will be able to select the right image in 68% percent of the time, advanced customers of level $\sigma 2$ will be able to select the right image in 95% of time, and exceptional customers will be able to select the right image in 98% of time. Initially, all customers are placed at

level 1 and will move to a higher level based on performance. A higher level means better skill. The stories presented to the user are divided into three groups *short*, *tall*, and *grande*. A short story consists of three pictures, a tall story consists of four pictures and grand story consists of five pictures. The system is designed in such a way that it is more difficult to find out the relation between five than between three pictures.

Table 2. Image selection probabilities vs. customer level and story level

Customer Level	Story	p_{00}	p_{01}	p_{02}	p_{03}
$\sigma 1$	short	0.997	0.003	0.8	0.2
$\sigma 1$	tall	0.95	0.05	0.8	0.2
$\sigma 1$	grande	0.68	0.32	0.8	0.2
$\sigma 2$	short	0.99936	0.00064	0.8	0.2
$\sigma 2$	tall	0.997	0.003	0.8	0.2
$\sigma 2$	grande	0.95	0.05	0.8	0.2
$\sigma 3$	short	0.99999942	0.00000058	0.8	0.2
$\sigma 3$	tall	0.99936	0.00064	0.8	0.2
$\sigma 3$	grande	0.997	0.003	0.8	0.2

A chain is no stronger than its weakest link. In the context of our system, the *weakest* link is actually the most *skillful* bad bot. The goal is to show that the system satisfies requirements in the worst-case scenario when attacked by the strongest and most skillful bad bot.

Table 3. The probabilities that web robot will select a correct image and be positively identified

Bot Level	Story	p_{00}	p_{01}	p_{02}	p_{03}
advanced	short	0.50	0.5	0.8	0.2
advanced	tall	0.40	0.6	0.8	0.2
advanced	grande	0.35	0.65	0.8	0.2

4 Model of the Subject

Assume the subject is human with the skill level of $\sigma 1$ and that *grande* story is presented to the subject. According to the data shown in Table 2 in 68% of the time the subject human will discover the right message. Next, the detector will with 80% of probability determine if the subject is human or bot. The model is shown in Figure 2. The event that represents image selection is shown by probabilistic transition *E0*. The transition has two alternatives: with probability p_{00} system goes into the state *Correct*, and with probability p_{01} to *Incorrect* state. The transition *E1* represents the event that evaluates the subject that can be either human or robot. With the probability p_{02} we assume that

the subject is human, and with probability p_{03} that the subject is a bot. Those estimations are based on the data acquired from mouse movements, and user agents. The probability that a human selects a correct image, and that system confirms that an image is selected by a human is

$$0.68 * 0.8 = 0.544 \tag{1}$$

As presented in Table 5 we call this *true positive* rate. The probability that a human detects the right image, but the system thinks the image is selected by a bot or *false positive* is

$$0.68 * 0.2 = 0.136 \tag{2}$$

An authentication process that positively identifies a user in little more than 50% of the time is not useful. To make this system practical, we decided to repeat the image selection test multiple times according to the model shown in Figure 3. With each iteration the probability of *true positive* detection rate increases, while *false positive* decreases.

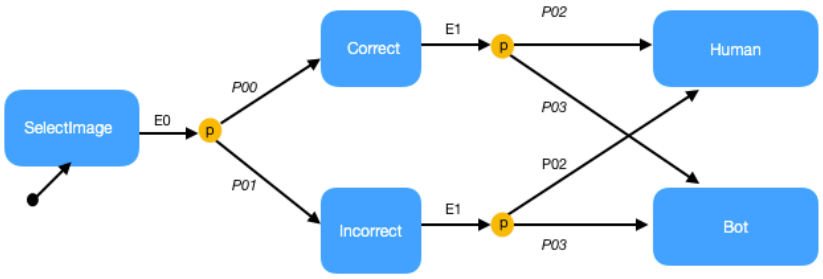

Fig. 2. Simple human authentication

4.1 Improved Model of the Subject

In the basic model, we show a one-shot authentication process. In this improved model, we repeat the process multiple times without changing the story difficulty level. It is a multilevel authentication approach. For a model given in Figure 3 we repeat authentication up to specified *MAX* number of times. For the purpose of this work, we fixed the maximum number of retries to five. We assigned a *reward* to each state to be used to reason about a wider range of quantitative measures relating to model behavior. For example, we can compute the expected number of transitions that pass through the *Correct* state.

In Figure 4 we show the expectation to visit any of states *Correct*, *Incorrect*, *Human*, *Bot* in each step. For instance, it is expected that in five steps customer $\sigma 1$ detects the correct image 4 times.

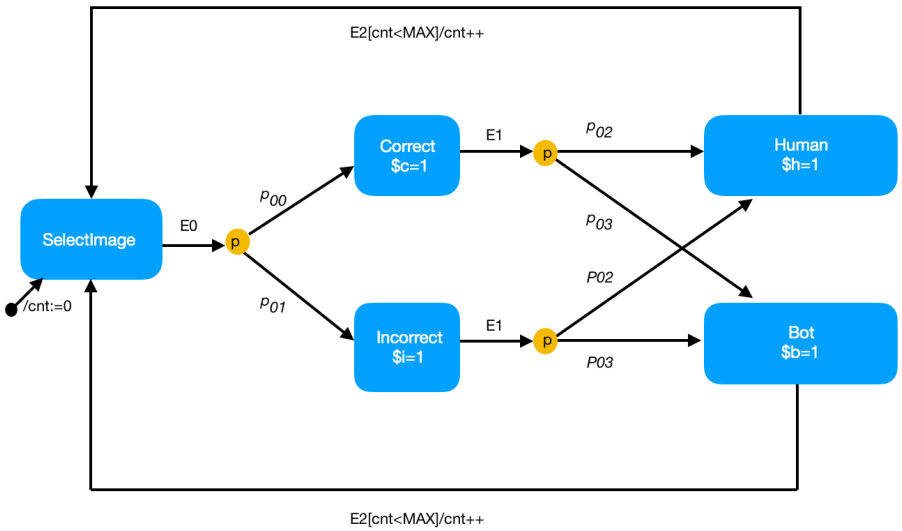

Fig. 3. Improved authentication - pCharts model

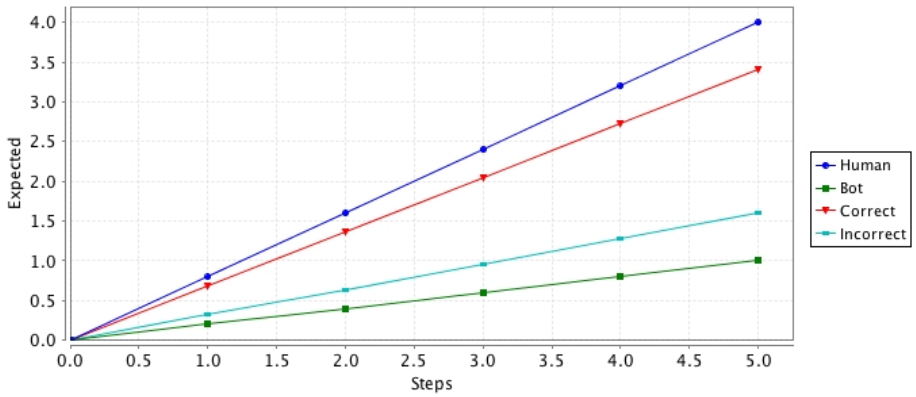

Fig. 4. Maximum expectations to go through a particular state for $\sigma 1$ customer

Those properties are calculated by probabilistic model checker PRISM [5, 8, 13]. The properties are calculated over a probabilistic computational tree logic (PCTL) reward formula

$$R\{"h"\}max = ?[F(root = SelectImage)\&(cnt = Step)] \quad (3)$$

Reward formula 3 calculates the costs of being in the state *Human*. The path property "F" is *eventually* or *future* operator. The state *costs* are specified according to pCharts [10] syntax. The notation "$\$h = 1$" at the state in Figure 3 means every time state *Human* is reached, the variable h will increase its value by a maximum 1. If the probability that the state is reached is p, $0 \leq p \leq 1$, h will increase for $\Delta = p * h$. The calculation for the other three states *Correct*, *Incorrect*, and *Bot* is done over similar formulae, and the result is shown in a graph in Figure 4.

Next, we wanted to estimate the probability of how many times the state *Correct* will be reached with respect to the number of authentication iteration steps. For instance, with the probability of %0.68 we can expect to reach a *Correct* state in one step. The probability that the state *Correct* is reached two times, in two steps is %0.462, and that the state *Correct* is reached only one time in two steps is %0.435. Those calculations are done over a PCTL formula

$$Pmin = ?[F(root = SelectImage)\&(cnt = Steps)] \tag{4}$$

Calculated values are shown in the Figure 5.

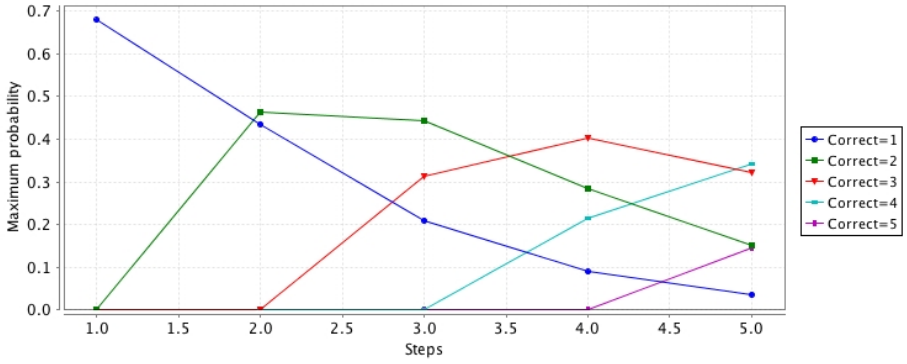

Fig. 5. Probability to have a particular number of *Correct* states in each step for $\sigma 1$ customer

Finally, over similar formula, we calculate the probability of how many times the state *Incorrect* will be reached with respect to the number of steps. Those calculations are shown on the graph in Figure 6.

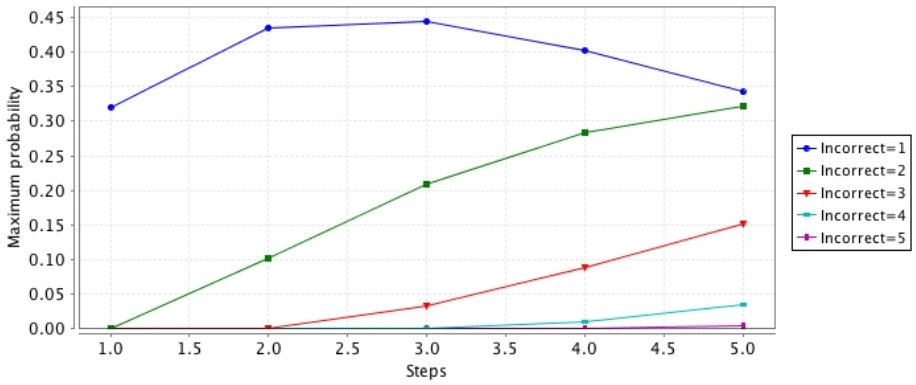

Fig. 6. Probability to have a particular number of *Incorrect* states in each step for $\sigma 1$ customer

Customer $\sigma 1$ is the least skillful and if the system can distinguish human from bot in %80 of time, even with repeated tests; it will be hard to positively identify the least skillful customer in the first three iterations. By repeating the process for more than three times we increase the probability of positive detection, but that may be inconvenient to the customer.

For more skillful customers $\sigma 2$ the probability to select the correct image related to *grande* story is 0.95 or 95% and for the most skillful is it 0.997 or 99.7%. Generated graph related to $\sigma 2$ and $\sigma 3$ customers are shown in Figures 7, 8, 9 and Figures 10, 11, 12.

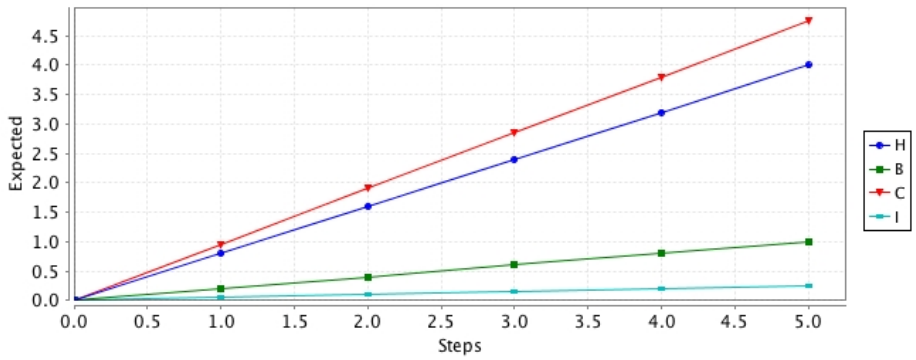

Fig. 7. *Expected*, $\sigma 2$

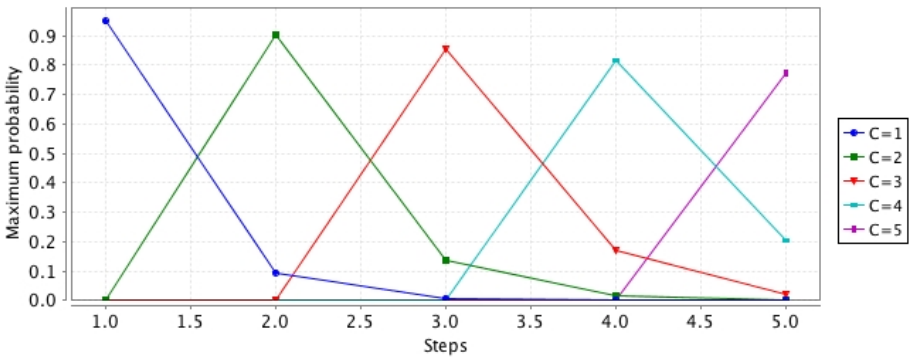

Fig. 8. *Correct*, $\sigma 2$

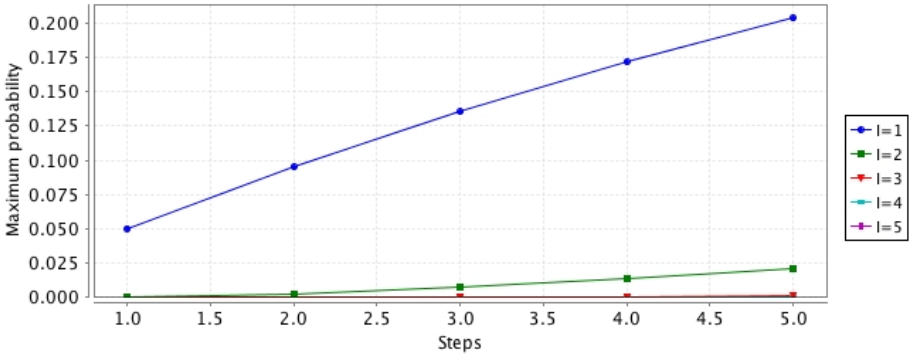

Fig. 9. *Incorrect*, $\sigma 2$

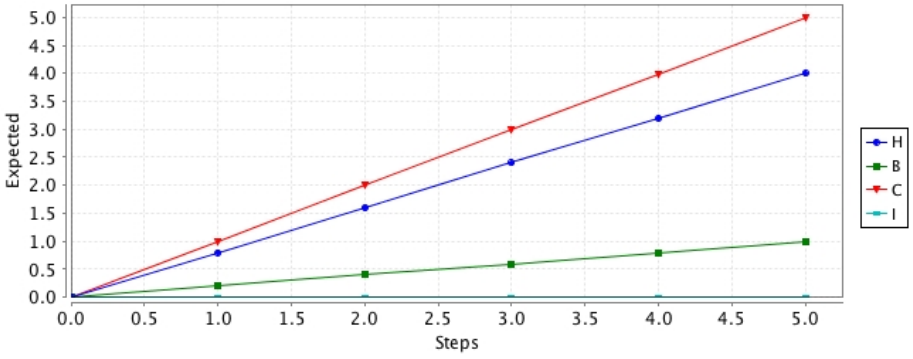

Fig. 10. *Expected*, $\sigma 3$

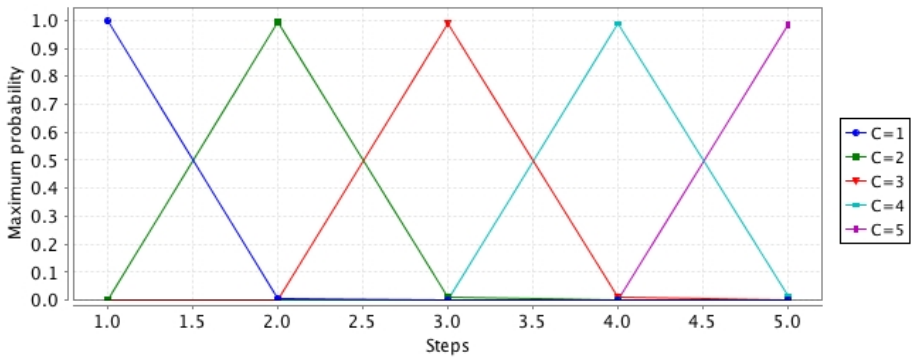

Fig. 11. *Correct*, $\sigma 3$

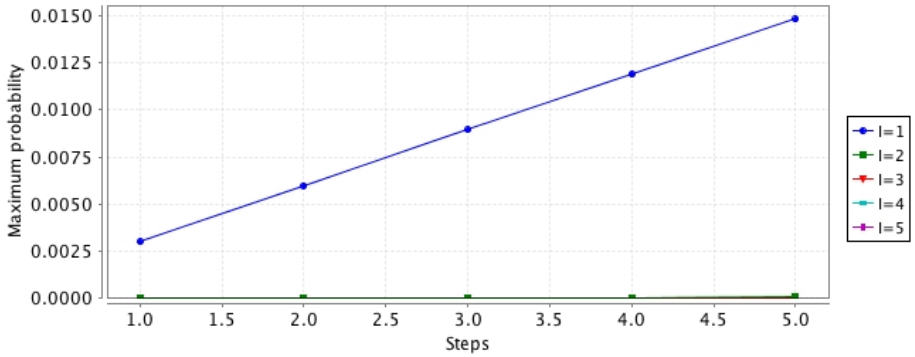

Fig. 12. *Incorrect*, $\sigma 3$

Web robot (bot) detection probability We assumed that the distinction between a bot and a human can be done at 80%. That is much smaller than 97.9% claimed in [3]. However, this number is usually not fixed - as the process of image detection becomes longer, the probability of bot detection increases. In a short period of time, a bot may learn how to behave like a human, but as time progress, it becomes more and more difficult for a bot to *hide* from the bot detection system. So we can model this probability with *exponential* distribution $1 - e^{-steps}$

Table 4. Bot detection probability - exponential

Step	1	2	3
Probability (p_{02})	0.63	0.86	0.95

Increasing bot detection in the model of subject human, will not have an effect on the number of visited *Correct* and *Incorrect* states as shown in Figures 5, 8, 11, 6, 9, and 12, but will have an impact on the Figures 4, 7, 10.

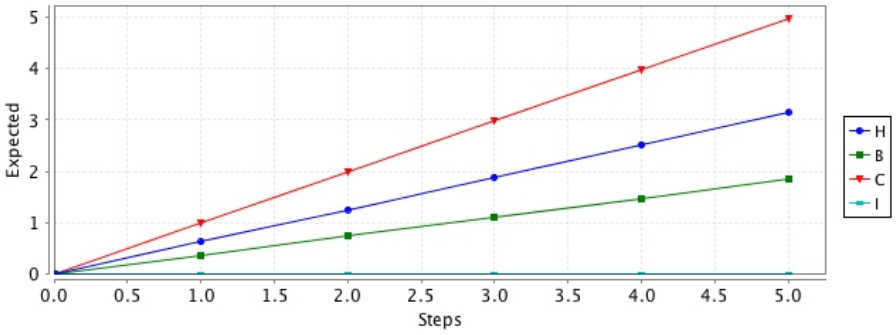

Fig. 13. $\sigma 3$, Step 1

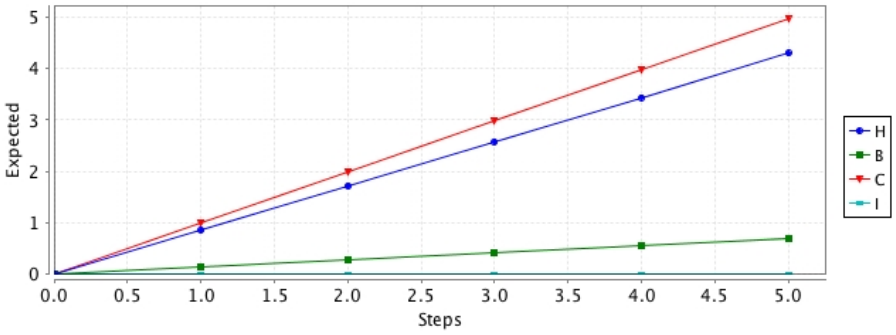

Fig. 14. $\sigma 3$, Step 2

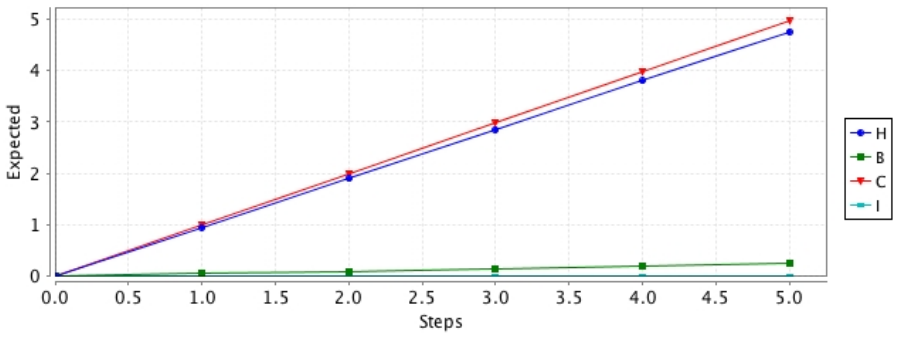

Fig. 15. $\sigma 3$, Step 3

As it is visible from Figures 13, 14, and 15 with each iteration the probability of true positive identification is increasing.

5 Future Work and Conclusion

The system gives only probabilistic output based on the provided data. Although the probability of *true positive* detection exponentially increases with each step it will never reach 100%. However, by adding ML we believe that we can further increase the probability of true positive detection.

The goal of ML is to recognize patterns from previous data for the purpose of making decisions or predictions. ML can be *supervised*, *unsupervised*, and *reinforcement* learning. Supervised learning is capable to solve a large class of problems in the area of classification and regression. In our study, we need to work on a classification problem to classify the observations into categorical discrete classes. Although it is possible to classify observation into four classes according to Table 5, we divide observations into two main classes: the class of *Miss* case and the class of all other cases. When the result of clarification has two discrete values, we call it binary classification.

The more data we provide to the ML system, the system becomes better, and consequently over time the system improves itself. The usefulness of ML in fraud detection is known, and for the purpose of our study, we tailored the model presented in [2] [12].

Table 5. Bot detection

True Positive - *Hit*	False Positive - *False Alarm*
False Negative - *Miss*	True Negative - *Normal*

The meaning of *true positive* is that when we believe that we detected it was really a bot. When the bot was present but not detected it is *false negative* case. We miss bad

bots and that comes with the most serious consequence. Another possibility is that a bot is detected and it was not a bot, we call this a *false positive*. This is also a so-called false alarm. It may create some inconvenience to the user, but there are no serious consequences. The last possibility is *true negative* when we did not detect a bot and it was not a bot. That is a successful situation. Following the example from [2], *false negative* rate is

$$\frac{Miss}{Hit + Miss} \tag{5}$$

and *false positive* rate is

$$\frac{False\ Alarm}{False\ Alarm + Normal} \tag{6}$$

Using the data for the worst-case scenario presented in the Section 4, we can figure out that the actual *false negative* rate with five retries is 0.032%. However the expected *false negative* rate is much smaller at $3.125 * 10^{-5}\%$ and in the best case it is $2.43\% * 10^{-11}$.

We believe that adding ML to the authentication process should become standard practice in future authentication systems. Inevitably bad bots are improving on a daily basis, so the system that protects against bad bots should continuously be improved, and this could mean incorporating ML features.

In this work, we use the probabilistic model checking approach to quantify the properties of the proposed online authentication process. We use the model to verify process feasibility. That implies qualitative verification and its quantitative evaluation. We show how those results can be used in the tune-up of our patent to make it more efficient. Our model shows that single authentication is not enough and that the authentication process has to be repeated multiple times. During this process, the ML feature of the authentication is crucial and gives additional credibility to the authentication process. It makes the process immune to aging since the process improves itself over time. Based on past successful authentication statistics, we quantify how confident we are that a user is who he claims to be.

6 Acknowledgment

I would like to give my thanks to Nebojisa Djosic, one of the inventors of an authentication technique based on image recognition. Special thanks to Ryan Shepard for his in-depth reading of the paper, excellent comments, and suggestions.

References

1. Canada, R.B.: Rbc online banking. `https://www.rbcroyalbank.com/personal.html` (February 2019)
2. Chan, P.K., Stolfo, S.J.: Toward scalable learning with non-uniform class and cost distributions: a case study in credit card fraud detection. In: KDD 1998 (1998)
3. Chu, Z., Gianvecchio, S., Koehl, A., Wang, H., Jajodia, S.: Blog or block: Detecting blog bots through behavioral biometrics. Computer Networks 57, 634–646 (2013)

4. Cresci, S., Pietro, R.D., Petrocchi, M., Spognardi, A., Tesconi, M.: Fame for sale: efficient detection of fake twitter followers. CoRR abs/1509.04098 (2015), http://arxiv.org/abs/1509.04098
5. Hinton, A., Kwiatkowska, M., Norman, G., Parker, D.: PRISM: A tool for automatic verification of probabilistic systems. In: Hermanns, H., Palsberg, J. (eds.) Proc. 12th International Conference on Tools and Algorithms for the Construction and Analysis of Systems. Lecture Notes in Computer Science, vol. 3920, pp. 441–444. Springer (2006)
6. Igal, Z.: Bot Traffic Report 2016. https://www.incapsula.com/blog/bot-traffic-report-2016.html (February 2019)
7. Khomh, F., Adams, B., Cheng, J., Fokaefs, M., Antoniol, G.: Software engineering for machine-learning applications: The road ahead. IEEE Software **35**(5), 81–84 (September/October 2018). https://doi.org/10.1109/MS.2018.3571224, doi.ieeecomputersociety.org/10.1109/MS.2018.3571224
8. Kwiatkowska, M., Norman, G., Parker, D.: Prism 4.0: Verification of probabilistic real-time systems. In: Gopalakrishnan, G., Qadeer, S. (eds.) Computer Aided Verification. Lecture Notes in Computer Science, vol. 6806, pp. 585–591. Springer Berlin Heidelberg (2011)
9. Morstatter, F., Wu, L., Nazer, T.H., Carley, K.M., Liu, H.: A new approach to bot detection: Striking the balance between precision and recall. In: 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM). pp. 533–540 (Aug 2016). https://doi.org/10.1109/ASONAM.2016.7752287
10. Nokovic, B., Sekerinski, E.: Verification and code generation for timed transitions in pcharts. In: Proceedings of the International C* Conference on Computer Science and Software Engineering. C3S2E '14, ACM, New York, NY, USA (2014). https://doi.org/10.1145/2641483.2641522, to appear
11. Oeltjen, J.: Authentication and machine learning: Taking behavior recognition to a new level. https://www.csoonline.com/article/3209917/identity-management/article.html (January 2017)
12. van Oorschot P. C.: Basic Concepts and Principles. In: Computer Security and the Internet. Information Security and Cryptography. Springer (April 2020). https://doi.org/10.1007/978-3-030-33649-3
13. of Oxford, U.: PRISM. http://www.prismmodelchecker.org/ (December 2012)
14. Research, B.: Global Multi-Factor Authentication Market: Trends and Forecast (2022-2027). https://www.reportlinker.com/p06364006/Global-Multi-Factor-Authentication-Market-Trends-and-Forecast.html?utm_source=GNW (November 2022)
15. Van Der Walt, E., Eloff, J.: Using machine learning to detect fake identities: Bots vs humans. IEEE Access 6, 6540–6549 (2018). https://doi.org/10.1109/ACCESS.2018.2796018
16. Villamarín-Salomón, R., Brustoloni, J.C.: Bayesian bot detection based on DNS traffic similarity. In: Proceedings of the 2009 ACM Symposium on Applied Computing. pp. 2035–2041. SAC '09, ACM, New York, NY, USA (2009). https://doi.org/10.1145/1529282.1529734, http://doi.acm.org/10.1145/1529282.1529734
17. Zhao, D., Traore, I., Sayed, B., Lu, W., Saad, S., Ghorbani, A., Garant, D.: Botnet detection based on traffic behavior analysis and flow intervals. Computers & Security 39 (11 2013). https://doi.org/10.1016/j.cose.2013.04.007