1.What do you know about authentication system (AS)?

1.1 What is AS?

Authentication systems (AS) are known as the first and last line of defense for any system. Most of the time, AS can prevent unauthorized users from accessing confidential data (Barkadehi et al., 2018, p. 1502).

1.2 What types of AS are available?

As of now, there are 4 types of Authentication System (AS) models available – Ownership, knowledge-based, inherent-based and mix models (see table 1 below).

Ownership model	Knowledge-based model	Inherent-based model	Mix models
1. Physical keys	1. Passwords	1. Fingerprints	1. Two factor
2. Smart card	2. PIN code	2. Palm	2. Multi-factor
3. NFC	3. Lock pattern	3. Iris	
4. RFID	4. Graphical password	4. Voices	
5. Hardware-token	5. Rhyme based	5. Gestures	
6. Cell-phone	6. Challenge response	6. Face	

Source: Barkadehi, N. (2018)

1.3 What is Typing Habit Gesture Authentication System?

This is a type of behavioral inherent-based authentication system implemented by recording patterns in a person's typing habit.

There are 2 types of typing habits: fixed and free text (Identifying Users Using Keystroke Dynamics and Contextual Information, 2018)

Fixed

The system prompts the user to repeatedly type the same predefined text several times. The predefined text is always the same. For example, the text could be a password, or a string consisting of your information such as: name, surname, login or password.

Free

The system will prompt the user to type long portions of text that mimics the concept of typing whatever they want without limitations. The system's algorithm makes use of this input to filter the necessary features and build a unique model for the user. The algorithm should determine the validity of the samples.

In this project, the team be focusing more on typing habits based on fixed texts on a regular computer (QWERTY) keyboard.

2. What do you understand about typing gesture habit?

Typing gesture habit has an alternative name which is also called as keystroke dynamics. Unlike other forms of biometric such as fingerprint scanning, iris scanning, and facial recognition, keystroke dynamics doesn't require an active input. Instead, keystroke dynamics analyzes user typing patterns, which may include typing rhythms, frequent mistakes, which shift keys used for capitalization and pace.

It creates a baseline for user typing and then uses the baseline to check for abnormalities. If an abnormality is detected, a different authentication factor may be requested to verify the user or to terminate the session immediately, depending on the security policy.

Keystroke dynamics fall under the category of "behavioral biometrics;" these use the behaviors of the users as an authentication factor. As such, hackers cannot "steal them" because they are integral to the personality of the users; they also cannot replicate them for the same reasons. So, instead of considering what words users' type, how they type becomes of special interest (Canner, 2020).

3. How typing gesture habit can be used for authentication? -terrence

According to Fabian Monroe and Aviel Rubin proceedings of the 4th ACM conference on Computer and communications security:

When a person types, the latency between successive keystrokes, keystroke durations, finger placement and applied pressure on the keys can be used to construct a unique signature for that individual. For well known, regularly typed strings, such signatures can be quite consistent. Furthermore, keystroke dynamics is not intrusive, making it very applicable to computer access security as the users will be typing at the keyboard anyway.

Unlike conventional passwords and PINs, behavioral typing gesture cannot be stolen or lost, and implementing it can serve as a safe and cheap way as it only requires a keyboard to achieve authentication.

4. Parameters of typing gesture

4.1 Text entry speed: Words per minute

Things to consider:

- When did the timing for a phrase begin?
- When did it end?
- Did timing begin with the first character or with a START button or some other signal before the first character?
- Did timing end with the last character or by pressing ENTER after the last character?
- If timing begins with the first character and ends with the last character, then, arguably, the first character should not count, since timing excludes the time leading up to the entry of the first character.

4.2 Accuracy / Error rate: ration of incorrect characters to total characters

Insertion errors & deletion errors may lead to accuracy problems and hence, might affect the recognition of the user.

4.3 Dwelling time: text entry by eye typing

Things to consider:

1. A study carried out in 1996 reported that “for people with severe disabilities it can take anywhere from 15 minutes to many months to acquire eye control skill to run the system.” (Tecce, 1998, p. 320). The speed of real experts has not been systematically measured for any of the eye-controlled text entry systems.

2. As another example, consider (Wigdor & Balakrishnan, 2005, p. 212) TiltText, a technique for mobile phone text entry that uses the orientation of the device to resolve the ambiguity of letters on keys on the mobile phone keypad. In addition to conventional error rate analyses, they defined and used “button error” and “tilt error” as dependent variables. Button errors were the ratio of errors due to pressing the wrong button, and tilt errors were the ratio of errors due to tilting the device in the wrong direction.

   PiePad is a gesture-based entry method for numeric entry (Quinn & Zhai, 2016, p. 235; (MacKenzie & Tanaka-Ishii, 2007, pp. 1–3). Gestures were stylus strokes conforming to a clock metaphor: right for 3, down for 6, left for 9, and so on. In addition to analyzing the time to make gestures, they defined and used “preparation time” and “scripting time” as dependent variables. Preparation time was the time between gestures, from stylus up after the previous character to stylus down for the current character. Scripting time was the gesturing time, from stylus down to stylus up.

3. Experiments have been performed with text entry by gaze using a common, “off-the-shelf” video camera with the GazeTalk system (Itoh et al., 2006, p. 65). They observed text entry speeds of 3–5 WPM by untrained users using large (3 × 4) on-screen buttons. It is not surprising that systems requiring hierarchical navigation or multiple gestures are slower than on-screen Qwerty keyboards with accurate eye trackers, although the prediction and completion features can improve the text entry speed. Their use depends heavily on both individual styles and extended use, so they are difficult to evaluate without longitudinal studies.

4. The language of the text also has an effect on text entry speed. All the figures given so far are for English. GazeTalk and Dasher also support entering text in Japanese. A study with the results on the typing speed of 22–24 Kanji characters per minute, with performance improving from 19 to 23–25 characters per minute over seven short trials over 3 days was also tested (Itoh et al., 2006, p. 65). Both systems reached these text entry rates.

5. What is AI?

Artificial Intelligence (AI) refers to the simulation of human intelligence in machines programmed to think like humans and to imitate their actions. The term can also be applied to any machine that exhibits features associated with a human mind, such as learning and problem-solving.

The ideal characteristic of artificial intelligence is its ability to rationalize and take action that has the best chance of achieving a specific goal. A subset of artificial intelligence is machine learning, which refers to the concept that computer programs can automatically learn from and adapt to new data without the assistance of humans. Deep learning techniques enable automatic learning through the absorption of vast amounts of unstructured data, such as text, images or video (Frankenfield, 2021).

An example of this is that Keystrokes generated maliciously that do not normally match human typing and can be easily detected. Using artificial intelligence, however, the Malboard attack independently generates user-style commands, injects keystrokes as malicious software into the keyboard, and avoids detection. The keyboards used in the research were the products of Microsoft, Lenovo and Dell.

"Our proposed detection modules are reliable and secure, based on information that can be measured from side-channel resources, in addition to data transmission," says BGU student Nitzan Farhi.

“These include (1) the keyboard’s power consumption; (2) the keystrokes’ sound; and (3) the user’s behavior associated with his or her ability to respond to typographical errors.”

Dr. Nissim adds, “Each of the proposed detection modules is capable of detecting the Malboard attack in 100% of the cases, with no misses and no false positives. Using them together as an ensemble detection framework will assure that an organization is immune to the Malboard attack as well as other keystroke attacks.” (Security, 2020).

6. What is machine learning?

Machine learning involves using algorithms to obtain statistical information on massive amounts of data. Data can come in many different forms such as numbers, words or even pictures. The uses of machine learning could be used to gain an advantage in marketing or showing recommendations on sites such as Google.

2 common methods of typing gesture authentication are fixed text or free text. Fixed text being a set paragraph that the user has to type and is predetermined by the system, or free text that is randomly generated by the system so each time would give different words. A machine learning algorithm requires training, by using supervised or unsupervised learning using new samples, before being used (Azevedo et al., 2007b, p. 69).

Supervised learning:

Datasets with a known result are used to train a model. The algorithm learns and adapts from the data provided to give results consistent with the provided results from the inputs. When an unknown sample is required to be evaluated, the algorithm can draw on what it has previously learned to provide and answer. The greater the number of samples used to train the model, the better it performs. Common methods of supervised learning algorithms include Support Vector Machine, Neural Networks and k-nearest neighbor.

Unsupervised learning:

This method does not know which samples to learn from as all data is unlabelled. The algorithm learns as samples are fed into it. A common method of unsupervised learning algorithms are Bayesian classifiers and clustering algorithms. The result can be ambiguous if the initial samples are misleading.

7. Software development methodologies, programming language and implementation.

We plan to implement our project with SCRUM methodology. With regular discussions with stakeholders and the using user stories, use case descriptions, class diagram, BCE diagrams, sequence diagrams to assist us in creating the framework of the whole program. With the use of Java programming language, we will be using GUI to create an interface for the user to input their data and using the concept of Object Orientated Programming to build our program.

8. Algorithm and implementation

“Keystroke dynamics is the detailed timing information that describes exactly when each key was pressed and when it was released when concrete person is typing at a keyboard of a computer, gadget etc.” (Kochegurova et al., 2017, p. 12073). In keystroke dynamics, features such as dwell time, intervals between key presses and overlapping of key presses are factors used to capture data. Dwell time is the time when a key is in

the pressed state. Intervals between key presses is period between two keys being pressed. Overlapping of keypresses is when 1 key is not released before another key is pressed, the increase of speed will cause a greater number of keys being overlapped.

How we apply it to our program is by having the user store their keystroke dynamics characteristics into a profile first. For the algorithm, we will be using Euclidean distance to use as comparison between the profile, stored with the user's keystroke dynamics characteristics and the current user's keystroke characteristics for authentication.

Euclidean distance can be calculated by:

$$P = \sqrt{\sum_{i=1}^{N} (t_{et} - t_{cur})^2}$$

where N – the amount of different characters,

t_{et} – the standard dwell time for a key;

t_{cur} – the current dwell time for this key.

Source: (Kochegurova et al., 2017, p. 12073)

9. Recent developments in the area and case studies

9.1 Bayesian regularized neural network

The authentication system was trained using fixed text to determine the user.

Method:

Their algorithm makes use of Bayesian regularized neural network trained using users' typing habits like *dwell time*, *flight time*, as well as total amount of time used to type password to record continuous keystroke dynamics data in different sessions on separate days. Dwell time refers to the time the user spent pressing the key, while flight

time refers to the interval or pause when the previous key is up, and the next key is pressed.

Operating environment:

This is a Java API-based application to be run on the computer on a basic keyboard. Upon startup, a screen is displayed where user is asked to enter username, session ID and their password. When users submit, the keystrokes are saved in the database. User is authenticated by their unique username and keystroke dynamics logged from sample text entered by that user (Zareen et al., 2018, p. 65).

9.2 Typing habit authentication system on android phone

Method:

The user is prompted to set their password and repeat it thirty times for the system to learn their typing pattern. The data provided by the user is fed into the system's artificial neural network. Then, weight function is applied on the network. Support Vector Machine (SVM) and K-Mean strategy is adopted to let the system learn to recognize users better. This authentication system makes use of three separate SQLite databases for these purposes: training values, saving password and storing trained weights from the artificial neural network (Mishra et al., 2018).

Operating environment:

This authentication system runs on android 5.0 (or later) consisting of components such as artificial neural network to keystroke values and authenticate user. The keystroke dynamics recorded are based on PIN and patterned passwords set by the user. The front-end user interface was written in JAVA and XML, while the database connected to the program was SQLite

9.3 Typing habit Authentication for banking transaction system

Method:

Registration

User is prompted to register their action (performing a banking transaction). During registration, user is prompted to input their password 10 times so that the keystroke dynamics are analyzed, and a threshold of the user's typing pattern is determined.

Login

User is prompted to complete their login process. Three tries will be given should they fail to log in. After account verification, the system authenticates the user by their keystroke habits. If the variance from the recorded typing pattern is little to none, full access will be given. Additionally, if variance is more than that but still within the threshold, partial access will be given to the user. Lastly, is variance recorded is past the threshold, no access will be granted.

Operating Environment:

The authentication system is a JAVA application is run on windows XP (or higher) with an SQL database (Chourasia, 2014).

References

1. Azevedo, G. L. F. B. G., Cavalcanti, G. D. C., & Filho, E. C. B. C. (2007b). Hybrid Solution for the Feature Selection in Personal Identification Problems through Keystroke Dynamics. 2007 International Joint Conference on Neural Networks, 67–72. https://doi.org/10.1109/ijcnn.2007.4371256.

2. Barkadehi, M. H., Nilashi, M., Ibrahim, O., Zakeri Fardi, A., & Samad, S. (2018). Authentication systems: A literature review and classification. Telematics and Informatics, 35(5), 1491–1511. https://doi.org/10.1016/j.tele.2018.03.018.

3. Canner, B. (2020, June 25). What are Keystroke Dynamics? How Can It Improve Your... Top Identity & Access Management Software, Vendors, Products, Solutions, & Services. https://solutionsreview.com/identity-management/what-are-keystroke-dynamics-how-can-it-improve-your-authentication/.

4. Chourasia, N. (2014, April 20). Authentication of the user by keystroke dynamics for banking transaction system. Https://Www.Digitalxplore.Org/. https://www.digitalxplore.org/up_proc/pdf/64-139807550041-45.pdf.

5. Frankenfield, J. (2021, January 6). How Artificial Intelligence Works. Investopedia. https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp.

6. Identifying users using Keystroke Dynamics and contextual information (No. 3). (2018). https://www.researchgate.net/publication/323028812_Identifying_users_using_Keystroke_Dynamics_and_contextual_information.

7. Itoh, K., Aoki, H., & Hansen, J. P. (2006). A comparative usability study of two Japanese gaze typing systems. Proceedings of the 2006 Symposium on Eye

Tracking Research & Applications - ETRA '06, 59–66. https://doi.org/10.1145/1117309.1117344.

8. Kochegurova, E. A., Gorokhova, E. S., & Mozgaleva, A. I. (2017). Development of the Keystroke Dynamics Recognition System. Journal of Physics: Conference Series, 803, 012073. https://doi.org/10.1088/1742-6596/803/1/012073.

9. MacKenzie, S. I., & Tanaka-Ishii, K. (2007). Text Entry Systems: Mobility, Accessibility, Universality (Morgan Kaufmann Series in Interactive Technologies) (1st ed.). Morgan Kaufmann.

10. Mishra, V., Gupta, R., Sood, G., & Patni, J. C. (2018). User Authentication using Keystroke Dynamics. Https://Research.Ijcaonline.Org/. https://research.ijcaonline.org/icrtstmsd2018/number1/icrtstmsd201806.pdf.

11. Quinn, P., & Zhai, S. (2016). Modeling Gesture-Typing Movements. Human–Computer Interaction, 33(3), 234–280. https://doi.org/10.1080/07370024.2016.1215922

12. Security, H. N. (2020, January 31). New user keystroke impersonation attack uses AI to evade detection. Help Net Security. https://www.helpnetsecurity.com/2019/06/10/user-keystroke-impersonation-attack/.

13. Tecce, J. (1998). Eye movement control of computer functions. International Journal of Psychophysiology, 29(3), 319–325. https://doi.org/10.1016/s0167-8760(98)00020-8.

14. Wigdor, D., & Balakrishnan, R. (2005). Empirical Investigation into the Effect of Orientation on Text Readability in Tabletop Displays. ECSCW 2005, 205–224. https://doi.org/10.1007/1-4020-4023-7_11.

15. Zareen, F. J., Matta, C., Arora, A., Singh, S., & Jabin, S. (2018). An authentication system using keystroke dynamics. International Journal of Biometrics, 10(1), 65. https://doi.org/10.1504/ijbm.2018.090129.