Original Article
ISSN (Online): 2456-8651

International Journal of Engineering Science Technologies
September-October 2025 9(5), 29–41

BIOMETRIC AUTHENTICATION MODULE TO ENHANCE CUBESAT SECURITY

Amina AlBalooshi [1], Ali AlMahmood [1]

[1] Satellite Design and Construction, Bahrain Space Agency, Bahrain

Received 15 August 2025
Accepted 17 September 2025
Published 04 November 2025

Corresponding Author
Amina AlBalooshi,
amina_a.hamid@hotmail.com

DOI 10.29121/IJOEST.v9.i5.2025.720

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

CubeSats suffer from limitations in power and processing capacity, often leading developers with limited options in implementing data security measures thereby increasing the vulnerability to data breaches and unauthorized access. These attacks negatively affected CubeSat operations or caused losing control over CubeSats in orbit; therefore, recent missions have prioritized the implementation of security measures, with data encryption being the most common method to defend against eavesdropping, and authentication protocols to prevent unauthorized access. This study presents an application of a Fuzzy Logic-based Authentication module to enhance CubeSats' security with minimal strain on the processing power of the Command and Data Handling System (CDHS) and without the need of additional hardware, targeting missions with constrained budgets relying solely on Commercial Off-The-Shelf (COTS) hardware. The module addresses cyber-attacks by analyzing the typing pattern transmitted during the initial communication, in addition to the username and password, such that authenticated users are granted access to the CubeSat. The success criteria defined in this study were based on two primary elements: (1) granting access to authenticated users with accurate credentials and (2) denying access for any user attempting impersonation, regardless of providing correct credentials. During initial testing, the algorithm achieved a 97% success rate in authenticating legitimate users, while maintaining an average 95% success rate in detecting impersonation attempts. These results will be verified after the launch of the CubeSat, where the algorithm will undergo further testing in real-time operations, as its performance is influenced by operators' behavior, which can vary significantly during actual use.

Keywords: CubeSat, Security, Authentication

1. INTRODUCTION

The historical event of Sputnik was revolutionary, the first satellite to be orbiting around Earth in the late 1950s marking the start of the space race. The event allowed rapid technological advancement in space systems, to the point where satellites became a very popular technology supporting different sectors such as agribusinesses, military, and transportation. This also includes any other sector that relies on space assets for accurate time and synchronization ranging from core network data transmission to the financial sector to energy distributors Falco (2019). However, despite all the advantages of satellites, the design complexity and cost required to develop and launch one, made it limited to large agencies such as the National Aeronautics of Space Administration, European Space Agency,

Roscosmos, or China National Space Administration. That is when the late 1990s marked the revolutionary design of CubeSats.

The footprint of CubeSats was highly impactful in further development of technologies used in space, and that was due to it being a powerful cost-effective vehicle that can host and test technologies. Its simplistic design and development process opened the doors to educational institutions, small agencies and even individuals to participate and contribute to space research. And throughout the years, it led CubeSats to gain rapid technological advancement allowing them to carry complex systems onboard making them very close in functionality to larger satellites. And as of January 1st, 2021, it was noted that 801 nanosats were in orbit with a development cost of only $25,000 to $40,000 and around $40,000 for launching services Falco (2019).

In recent years, CubeSats became accessible due to the many Components-of-the-shelf (COTS) available in the market, and with enough simplicity, it allowed young adults to participate in space exploration and research. Those little boxes contained powerful components allowing them to gather massive amounts of data throughout their lifetime, and although most are insensitive information, some contain information that can threaten countries' national security. Therefore, it is crucial for CubeSats nowadays to contain some sort of data security to defend against advanced cyber-attacks.

Cyber-attacks can jeopardize the data of the system; this increases the significance of having data security, whether on terrestrial systems or CubeSats in orbit. This is when space security became a trending topic among technical professionals and policy makers, particularly, after the increased launch of CubeSats without counting for their security Falco et al. (2021). And it was noticed that despite the exceptional advancement in the space industry, cybersecurity on the other hand, stayed outdated in relevance to other high-technology sectors Falco (2019). This made CubeSats with very minimal security mechanisms prone to different cyberattacks, namely: Denial of Service (DoS), data tampering, or disabling the CubeSat Challa et al. (2012).

In Denial-of-Service attacks (DOS/DDOS), attackers consume all satellite communication and processing resources, disrupt the state of information, disrupt network components, or disrupt the communication path. On the other hand, masquerade and unauthorized access attacks, allow attackers to obtain unauthorized control over the satellite and impersonate authorized operator. These security breaches allow attackers to perform incorrect health and status actions, in addition to sending unauthorized commands, leading to the prevention of authorized access to the satellite, damage, data loss, or loss of the satellite CCSDS Secretariat (2006). An example of the very early attacks, when ROSAT X-Ray satellite turned its solar panels towards the sun, due to a cyber-attack, where this action destroyed all sensors on the satellite. However, due to the nature of space systems and satellites, cyber-attacks can go undetected or seem like natural failures Falco et al. (2021).

Confidentiality, integrity and availability are the three main components of data security. Confidentiality refers to the property of the data that it can only be read by the authorized personnels, while integrity refers to the property of which the data is valid and is usually a concern with the data transmission. Finally, availability, and hence the name, refers to the property that the data is available when requested Challa et al. (2012). Some implementation of cybersecurity includes encryption and authentication, where the former is the adoption of optimized algorithms to provide

confidentiality of the generated data, while the latter provide a layer of protection against unauthorized access of controlling and operating the system.

The proposed frameworks in the literature provided unique solutions on cyber security for CubeSats, with a predominance in the reliance on encryption or authentication.

The framework designed by Challa et al. (2012). took into account the constraints of CubeSat which include but are not limited to power, size, weight and communication time. With those constraints, the software vs. hardware implementation of block ciphers was also studied, and it was concluded that software implementation on CubeSat is resource intensive and time consuming. Therefore, the authors analyzed several micro-controllers and settled for the ATXMega128 due to having block cipher hardware support, specifically to Advance Encryption Standard (AES) and Data Encryption Standard (DES). The system surpassed the constraints of CubeSat, where the size, weight and power requirements are within the limits of a CubeSat where it contains two microcontrollers with a total size of less than 5x5 cm and a total wight of 9.6g requiring only 2.4 mW. The microcontroller was able to achieve a 256 Kbps encryption speed, though, the microcontrollers are configurable, if needed, through clocking one of the controllers to a higher speed using more power. It is also possible depending on the requirement that the size, weight and power be traded off at the cost of the other. The framework can be installed in any CubeSat, providing a high level of data security through the adoption of Advanced Encryption Standard (AES) and Data Encryption Standard (DES) block encryption algorithms.

Ghandour and Abdallah (2018). developed an anomaly-based intrusion prevention system, which is designed and implemented on LibanSat. The system proposes a security protocol designed for CubeSats, the Intrusion Prevention System copes with the power and mass limitations, and the baseline state is defined as a networks' traffic load, protocol used, and regular package size. The anomaly detection agent on-board the CubeSat monitors received packets for baseline misuses, if any misuse is detected, the anomaly agent drops the packets. If a single transmitter is detected to have five misuses, it is then added to a block list.

Almazrouei et al. (2021). developed a security mechanism as part of the operating system on the on-board the main controller, the mechanism runs user authentication, utilizing username-password user credentials with three privilege levels: user, superuser, and manufacturer. Users are permitted to run normal operations (downloading data), superusers are allowed to run some of the configuration commands in addition to the normal operation commands, and all commands can be executed by manufacturers.

Mathews (2021). developed a unique framework that produces a randomly generated key through the random bit flips in the Random Access Memory (RAM) that occur during SEU. SEU are events that occur at random and are caused by ionizing radiation that when passed through, the electronics may cause the state of the bit to be flipped. It was estimated that the rate of bit flips that occur per day is around 10 at a cross section of 10-11 cm2 per bit. And to simulate the same degree of randomness produced by those SEU, Cryptographically Secure Pseudo-Random Number Generators (CSPRNGs) were used as part of the process in the generation of the key. It can be summarized as follows: the Random Access Memory (RAM) addresses are initialized with non-zero values and are monitored with Cyclic Redundancy Checks (CRC) until a bit flip occurs. The Random Access Memory (RAM) addresses are read and used as the seed for the 12-bit Linear Feedback Shift Register (LFSR), such that tapping is conducted according to the multiplexer value specified

and the key is generated. Those generated keys were then used as an input for the National Institute of Standard and Technology (NIST) testing suit and passed 11 of the 14 tests. The authors find the proposed design to be inconclusive at the time of writing the paper, however, provided several points to be followed such that it can be implemented to CubeSat missions:

- Test the CubeSat in its entirety and not only through software simulation.
- Investigate the effect of the proposed design on the thermal profiles of the CubeSat.
- Investigate the integration of the proposed design with CubeSat subsystems such as the Command and Data Handling and Communications.

Although, these frameworks offer excellent enhancement to CubeSat security, they can be inaccessible for educational missions using COTS or missions operating within tight budget constraints. Additionally, CubeSats with 1U or 2U configurations, incorporating additional hardware besides the main systems into the CubeSat stack is usually infeasible. In this paper, we present a Biometric User Authentication module that implements a fuzzy logic computing approach to identify users' typing rhythm and can distinguish between authorized and unauthorized users during the operation of a CubeSat. The module is being hosted and tested on a LEO CubeSat mission; however, it will not be incorporated with the flight software as its for-testing purposes only. Acquiring flight heritage of the module will provide light and efficient layer of security against spoofing attacks for future missions.

And while biometric authentication is commonly employed across various systems, especially in our daily-use devices, it was observed that there is an absence of its integration in small satellites, particularly CubeSats. The novelty of our application provides a lightweight, efficient and accessible module to augment CubeSat missions with an added layer of protection that enhances the username/password type of authentication, without imposing excessive demands on the processing power of the CDHS.

The rest of the paper is structured in the following manner: Section II provides the different data security solutions that other CubeSat developers are utilizing to ensure CubeSat remains confidential and safe against different attacks. Section IV outlines the methodology employed during the development of the framework. Section V presents the implementation of the methodology. Last but not least, Section VI provide a brief of the paper and providing conclusion remarks regarding the implementation of the module while also proposing possible enhancements to the module.

2. MATERIALS AND METHODS

The methodology followed in this research is divided into five main stages: User Identification, Profile Creation, Login Data Collection, Fuzzy Logic Function, and Verification. Prior to conducting the study, all participants were provided with detailed information about the study's purpose, the types of biometric data collected, and how their data would be used. Informed consent was then obtained from each participant, allowing their data to be used throughout the study.

All participants prior to their involvement in this study was given detailed information regarding the purpose of this study, the type of biometric data collected, and how their data would be used. Accordingly, informed consent was obtained.

2.1. USER IDENTIFICATION

The aim of this research can be reached through monitoring the user's typing behavior through the registration process. The user is required to select their credentials by choosing a unique username and a password that fits the security requirements; where password needs to have a minimum of one capital character, number, and special character, and a size of 8-20 characters. And with reference to the Central Limit Theorem; the typing pattern is captured with a sampling size of 30 entries such that the distribution of the sample is approximately normally distributed Masum (2022).

The typing pattern is constructed by capturing three elements, namely: Flight Time, Total Time, and Special Characters. The flight time, as shown in Figure 1 is defined by the time between two consecutive key presses, if a user has a password starts with "A1b2" and ends with "#" with a length of n, the first flight time recorded is the time duration from pressing "A" to "1". Likewise, the Flight time is collected for all key presses; thus, the total number of readings for the flight times collected is equal to the password size.

The total time for each of the 30 password entries is collected starting from the first character till the user presses the "enter" key. If a user has a password that starts with "A1b2" and ends with "#" with a length of n, the total time is collected from key "A" till the last key "enter" Figure 1. Finally, special characters' behavior is captured, whether the user is using "caps lock" or "shift" to switch letters to capital.

Figure 1

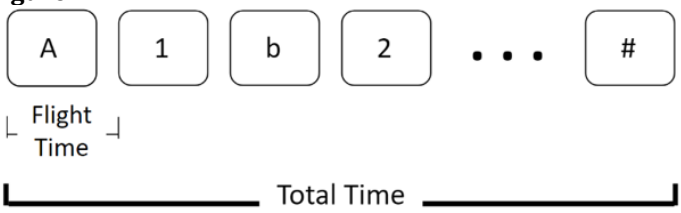

Figure 1 Keystroke Flight Time and Total Time

After the successful completion of this stage, the data collected is as follows:

- **Username:** The unique username selected.
- **Password:** The password selected.
- **Typing Time Array:** A two-dimensional array containing the key flight time of the 30 entries collected. Where each row presents a single try and columns present the character flight time.
- **Total Time Array:** A one-dimensional array containing the total time of the 30 entries collected.
- **Special Characters:** A flag representing the utilization of special character "Caps Lock" or "Shift".

2.2. PROFILE CREATION

The stage of profile creation analysis Typing Time Array and Total Time Array, by determining the minimum, average, and maximum values. For each column (Flight Time) the minimum, average, and maximum values are calculated, and constructed into three one-dimensional arrays Figure 2 Similarly, the same

operation is applied on the total time array, resulting in minimum total time, average total time, and maximum total time.

Figure 2

	Flight Time [0]	Flight Time [1]	...	Flight Time [*n*]
Attempt 1				
Attempt 2				
Attempt 3				
...				
Attempt 30				
Minimum	Minimum T[0]	Minimum T[1]		Minimum T[*n*]
Average	Average T[0]	Average T[1]		Average T[n]
Maximum	Maximum T[0]	Maximum T[1]		Maximum T[n]

Figure 2 Profile Creation Process

The resulting user profile Figure 3, where the data can be stored on devices that shall authenticate users.

Figure 3

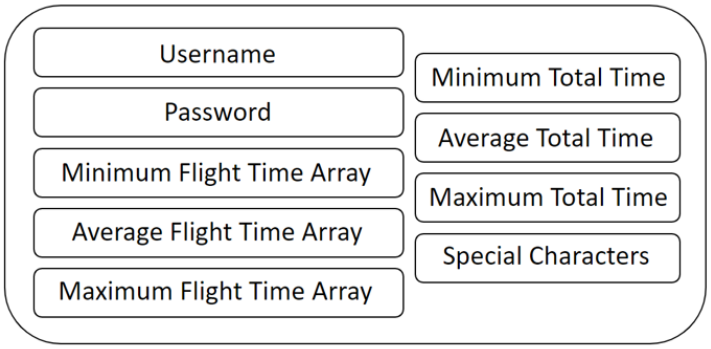

Figure 3 User Profile

2.3. LOGIN DATA COLLECTION

The login data is collected by monitoring user's typing behavior, the typing pattern is constructed, including the critical data needed for the different authentication levels and it consists of the following data:

- **Login Username:** The login username.
- **Login Password:** The login password.
- **Login Typing Time Array:** A one-dimensional array containing the key flight time of the user login password typing.
- **Login Total Time Array:** A variable containing the total time the user took to type the password.
- **Login Special Characters:** A flag representing the utilization of special character "Caps Lock" or "Shift".

2.4. FUZZY LOGIC FUNCTION

The fuzzy logic with triangle membership function, uses three parameters a, b, and c, where a and c define the base of the triangle and b the height of the triangle Figure 4.

Figure 4

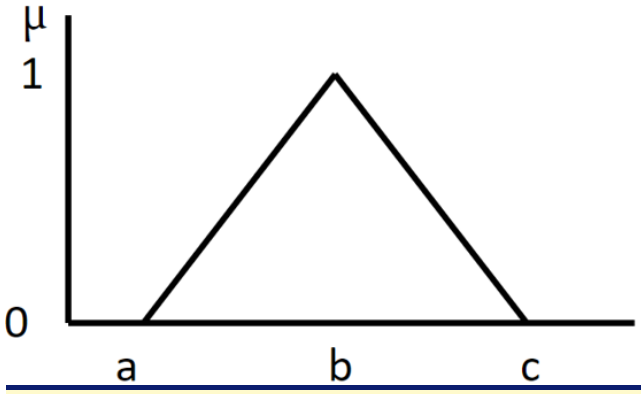

Figure 4 Triangle Membership Function

In the model the x-axis represents the input of the function, and the y-axis represents the corresponding fuzzy value CodeCrucks. (2021). The fuzzy value for each input is determined as follows:

- An input value equal to "b" will have a full membership value of 1.
- An input value less than "a" will have a value of 0.
- An input value greater than "c" will have a value of 0.
- An input value between a and "b" will have a membership value from 0 to 1, the closer the value is to b, the higher its membership value. eq. 1 shows the computation of this condition.

$$\mu(x) = \left(\frac{x-a}{b-a}\right), a \leq x \leq b \quad (1)$$

An input value between b and “c” will have a membership value from 0 to 1, the closer the value is to b, the higher its membership value, eq.2 shows the computation of this condition.

$$\mu(x) = \left(\frac{c-x}{c-b}\right), b \leq x \leq c \quad (2)$$

The final equation of the model is shown in eq.3.

$$x = \begin{cases} 0 & x \leq a \\ \mu(x) = \left(\frac{x-a}{b-a}\right) & a \leq x \leq b \\ \mu(x) = \left(\frac{c-x}{c-b}\right) & b \leq x \leq c \\ 0 & c \leq x \end{cases} \quad (3)$$

In this research, the fuzzy logic model is utilized to verify the login input data: Flight Time Array and Total Time, where the minimum and maximum values for each variable are the base of the triangle and the average is the height of the triangle Figure 5. The resulting equation is shown in eq.4.

$$x = \begin{cases} 0 & login \leq min \\ \mu(x) = \left(\frac{login - min}{avg - min}\right) & min \leq login \leq max \\ \mu(x) = \left(\frac{max - login}{max - avg}\right) & avg \leq login \leq max \\ 0 & max \leq login \end{cases} \quad (4)$$

In the case of the Login Flight Time Array, the fuzzy values of each Login Flight Time are calculated based on the triangle membership function that is constructed based on the minimum, average and maximum Flight Time Arrays. This results in a one-dimensional array of the fuzzy values calculated, in which the average (Flight Time Score) is then determined to be used in the next step (verification) of the authentication process.

Figure 5

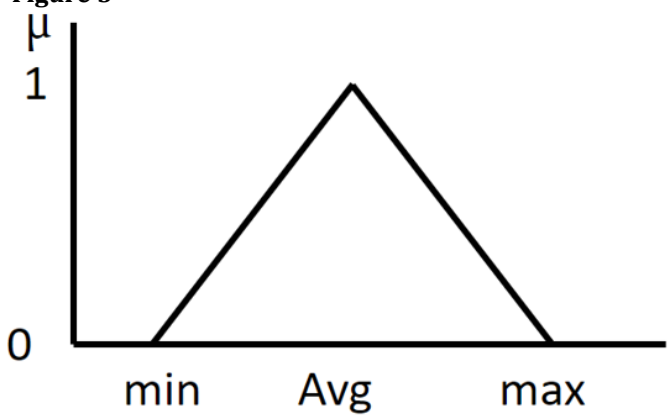

Figure 5 Authentication with Triangle Membership Function

Similarly, the fuzzy value of the Login Total Time is calculated based on the triangle membership function, and constructed using the minimum, average, and maximum Total Time. This results in the Total Time Score which is also used in the next step (verification) of the authentication process.

2.5. VERIFICATION

The verification process is to finalize the authentication decision of granting user access or denying it, by combing the different authentication factors. The results of the different authentication factors are multiplied with their corresponding impacts, then the total authentication score is calculated as per eq.5.

$$Score = I_0 \cdot R_0 + I_1 \cdot R_1 + .. + I_n . R_n \quad (5)$$

In this research the verification process is dependent on three factors: Flight Time Score (FT), Total Time Score (TT), and Special Character Flag (SC), where the Final Score function becomes as per eq.6.

$$Score = I_{FT} \cdot FT + I_{TT} \cdot TT + I_{SC}.SC \quad (6)$$

The authentication scores fall between 0 and 1, and it is granted access when the score is higher than the acceptance value.

2.6. IMPLEMENTATION OF THE METHODS

The authentication algorithm is customized for CubeSat missions so that the typing pattern is captured through the ground station software and uploaded to the desired CubeSat, where the CubeSat operation is granted or rejected. In the hosted mission, the algorithm will not block any command during the operation as it is implemented merely to test its functionality, reliability and practicability, thus eliminating the risk of false negative blocking of the operation. However, if the algorithm was determined successful in this mission, it shall be implemented as two-factor security for future missions since it provides a feasible solution with minimal complexity in improving CubeSat security. Acquiring flight heritage of the module would potentially lead to its adoption as a two-factor security measure for future missions.

The ground station software user interface and design were programmed using Windows Presentation Foundation (WPF) that is linked to a database. The software handles all the nominal operation of a ground station and provides additional features including a login and registration platform for the purpose of this mission which includes a registration and login platform, and all the data (CubeSat data and user entries) shall be stored within the database.

At the launch of the software, new users/operators are asked to register through the two-step registration process. In the first step, the user is required to fill in the username and password boxes, which upon confirmation, takes the user to the second step which includes retyping the password 30 times. During each typing attempt, and on the first keypress, the application starts a stopwatch in the backend that will capture the keystroke flight time and total time until the last keypress. In addition, the application captures the special keys pressed while typing the password (Caps Lock or Shift Key).

Once the 30 entries are successfully captured, the data is analyzed, where the total time, and keystroke flight time minimum, average, and maximum are calculated. The registration process is considered complete if, and only if, the two steps are successful, in which the user profile is created and saved to the database.

Users and Operators get access to the ground station software through their login credentials and are required to start each operation with an initialization command. During the login process the ground station software captures the user's typing pattern, and it is attached to the command that is transmitted to the CubeSat.

The CubeSat software is developed using c-programming language on the payload controller, and the process is initiated once a ground station command is received initializing the start of communication with the ground station. Once the command is received, the payload controller software sends a request to the database to search for the username received, as shown in Figure 6 If the user is

found, the database will retrieve all related data to the flight software for the authentication process.

Figure 6

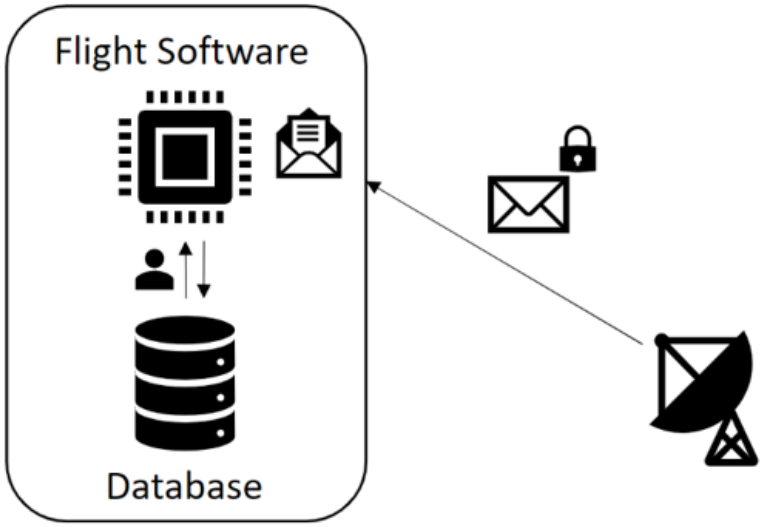

Figure 6 Authentication Process

3. RESULTS AND DISCUSSIONS

As part of the preliminary results, we conducted an initial evaluation to test the performance of the algorithm using a number of ground station operators and a number of non-registered users. This small-scale test served as the basis for validating the effectiveness of the algorithm, the results for two legitimates users are presented in Figure 6 and Figure 7 Where first user was able to successfully login 97% of the time, and the second user as shown in Figure 8 was able to successfully login 95% of the time.

Figure 7

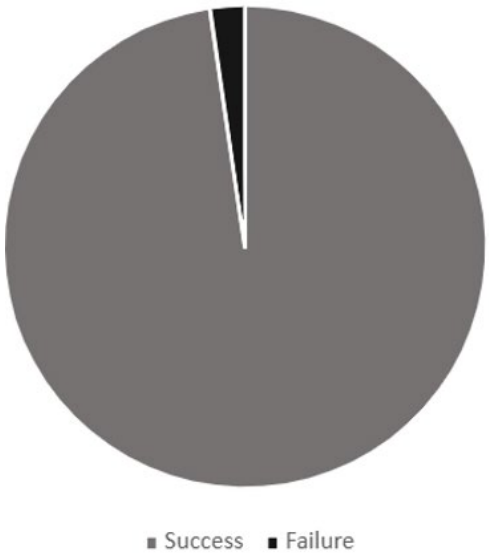

Figure 7 First User Login Success Rate

Figure 8

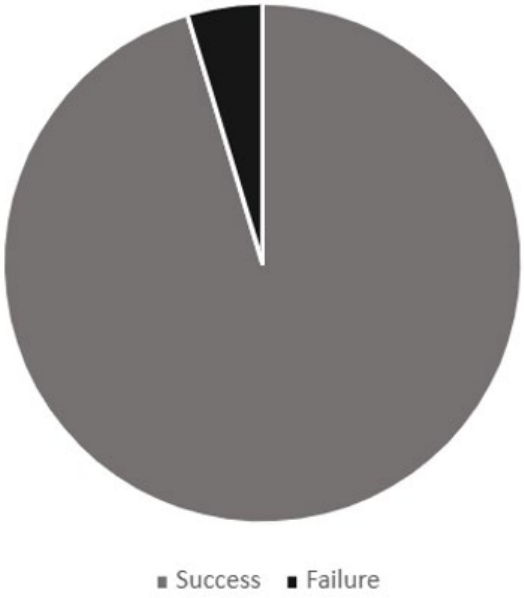

Figure 8 Second User Login Success Rate

Additionally, Figure 9 shows multiple trials, where each trial consisting of 30 attempts conducted by legitimate users and intruders to access the same account. Results show a clear difference in the number of times the legitimate user was able to successfully log in compared to intruders. These initial findings provide a foundational understanding of the algorithm's behavior in a real-world scenario.

Figure 9

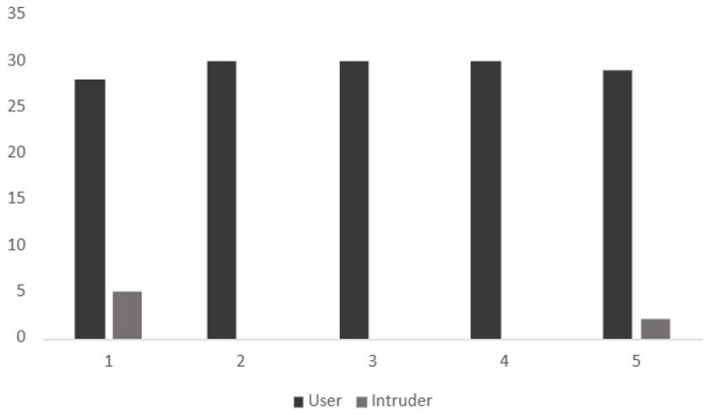

Figure 9 User and Intruder Login Attempts

4. CONCLUSIONS AND RECOMMENDATIONS

This paper has presented a Fuzzy Logic model-based authentication module in a CubeSat mission to enhance its security and defense against cyber-attacks, in particular, spoofing. The presented module utilizes the typing pattern besides the username and password to grant or reject a user from acquiring permission to operate the CubeSat, i.e., authorization is granted based on two conditions: (1) username/password match, and (2) the verification score is higher than the predetermined acceptance score. As aforementioned, each user profile was created

by collecting 30 login samples, saved in a database, where the data collected is utilized during the CubeSat operation.

The success of the module was defined as: (1) Access is given to the authenticated users who provide correct credentials and (2) Access is denied to any user impersonating another, even when providing the correct credentials. The module was tested during the development phase based upon the two success criteria, and the preliminary average success rate of authenticated user successful logins was 97%. While the average success rate to detect impersonated users was 95%.

It must be acknowledged that a degradation of the performance with the introduction of the space environment is expected when the CubeSat is in orbit. This is mainly because of the errors resulting from the RF communication channels and data buses onboard. In addition, the module can also be affected by the SEU such as bit flips. However, the module accuracy can be improved by considering a more complex verification algorithm, that may consider more variables to create user profiles, or a more complex mathematical model other than the Triangular membership function.

Most importantly, the implementation of the module does not require any additions of hardware nor demands high processing power of the CDHS. Making it a viable, and accessible option for CubeSat missions operating on a tight budget.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Almazrouei, A., Khan, A., Almesmari, A., Albuainain, A., Bushlaibi, A., Al Mahmood, A., AlBalooshi, A., et al. (2021). A Complete Mission Concept Design and Analysis of the Student-Led Cubesat Project: Light-1. In Proceedings of the Aerospace Engineering Conference 2021. https://doi.org/10.3390/aerospace8090247

CCSDS Secretariat. (2006). Security Threats Against Space Missions (Green Book, Issue 1). Consultative Committee for Space Data Systems (CCSDS).

Challa, O., Bhat, G., & McNair, J. (2012). CubeSec and GndSec: A Lightweight Security Solution for CubeSat Communications. Paper Presented at the 26th Annual AIAA/USU Conference on Small Satellites, Logan, UT.

CodeCrucks. (2021, August 10). What is Fuzzy Membership Function—A Complete Guide. CodeCrucks.

Falco, G. (2019). Cybersecurity Principles for Space Systems. Journal of Aerospace Information Systems, 16(2), 61–70. https://doi.org/10.2514/1.I010693

Falco, G., Viswanathan, A., & Santangelo, A. (2021). CubeSat Security Attack Tree Analysis. In 2021 IEEE 8th International Conference on Space Mission Challenges for Information Technology (SMC-IT). https://doi.org/10.1109/SMC-IT51442.2021.00016

Ghandour, A., & Abdallah, M. (2018). Design of a Lebanese Cube Satellite. In Proceedings of the 2nd International Electronic Conference on Remote Sensing. https://doi.org/10.3390/ecrs-2-05135

Masum. (2022, February 15). Effect of Sample Size in Central Limit Theorem. Medium.

Mathews, M. (2021). Using Bit Flips as a Source of Randomness in CubeSat Communication Encryption. Acta Astronautica, 186, 546–549. https://doi.org/10.1016/j.actaastro.2020.11.036