An IoT-fuzzy based password checker system for wireless video surveillance system

Mohammed Ahmed Jasim, Tayseer Salman Atia
Department of Computer Engineering, Al Iraqia University, Baghdad, Iraq

Article Info

Article history:

Received Jul 7, 2022
Revised Aug 8, 2022
Accepted Aug 25, 2022

Keywords:

Fuzzy inference system
Fuzzy logic
IoT
Password
Video surveillance system

ABSTRACT

Wireless video surveillance systems (WVSS) are deployed in large environments for use in strategic places such as town centers, public streets, and airports and play an essential role in protecting critical infrastructure. However, WVSSs are vulnerable to unauthorized access due to weak login credentials, which leads to their exploitation to launch cyberattacks on other systems, such as distributed denial-of-service attacks. Hence, it is essential to secure these systems from unauthorized access. This paper proposes the Mamdani fuzzy inference system (FIS)-based password checker algorithm to estimate the password strength ratio (PSR) of internet protocol (IP) cameras and internet of things (IoT) devices. This algorithm composes three stages, the password extraction stage, which evaluates the input parameters of FIS from the real-time streaming protocol (RTSP) protocol using a counter of password characters. Then, the processing stage uses Mamdani FIS to optimize the input parameters to calculate the PSR. Finally, the alarm stage will notify the system administrator about weak IoT nodes. Unlike the existing approaches, this algorithm improves detection accuracy by informing the system administrator about threatened nodes. Extensive experiments are carried out to determine the efficiency of the proposed algorithm. The results confirm the efficiency of the proposed algorithm with high accuracy, which outperforms existing schemes.

Corresponding Author:

Mohammed Ahmed Jasim
Department of Computer Engineering, Al Iraqia University
Saba’a Abkar, Baghdad, Iraq
Email: mohammed.a.jasim@students.aliraqia.edu.iq

1. INTRODUCTION

The internet of things (IoT) is a concept that represents connected objects and devices of all types over the wired or wireless internet with an expanded ability to communicate with each other to perform a variety of functions [1]. In this context, sensors on IoT devices provide a continuous connection between the devices and the physical environment. Indeed, modern IoT devices have a set of sensors (e.g., microphone, light sensor, accelerometer, and so on) that enable more efficient and user-friendly applications [2].

Wireless video surveillance systems (WVSS) based on IoT are becoming increasingly popular recently. The government, private organizations, residential societies, and public spaces use it to monitor different activities for security and safety [3]. WVSS has the advantages of remote and continuous monitoring [4]. The use of internet protocol (IP) based wireless closed-circuit television (CCTV) cameras is growing popular in the current context [5]–[8] due to technical aspects such as flexibility, ease of use, and cost. WVSS employed in a variety of applications all over the world. Over several decades, surveillance technology has progressed from analog to packet switching systems (over IPv4 & IPv6 networks). Furthermore, because of the widespread and popular IoT, WVSS has become affordable. As a result, the market for security equipment in connected homes has increased by 36% in recent years [9]. Because of their persuasion, practicability, and affordability, WVSS have become commonplace in our daily lives. WVSS have become commonplace in our daily lives.

WVSS source nodes consist of IP cameras, a transceiver, storage, a central processing unit (CPU), and a power supply. Each node performs video compression, data transfer, and video capture as a fundamental function. In addition, each wireless node's CPU and transmission unit handle a large amount of video data without compromising information and security, which is a problematic issue in WVSS applications [10]. Figure 1 illustrates the overall architecture of a functional WVSS.

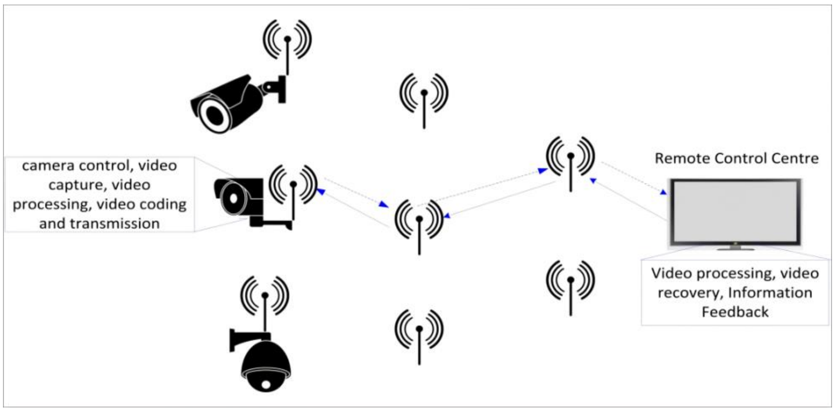

camera control, video capture, video processing, video coding and transmission
Remote Control Centre
Video processing, video recovery, Information Feedback

Figure 1. Overview of wireless video surveillance system [8]

These systems are vulnerable to unauthorized access attacks resulting in privacy and security issues; French web host OVH was exposed to distributed denial of service (DDoS) attack-Mirai [11] in September 2016, which was the most significant DDoS attack ever recorded. The source of the junk traffic was a botnet made up of 145,607 hacked digital video recorders and IP cameras, with the ability to generate traffic of 1 mbps to 30 mbps from every single IP address. This botnet can launch DDoS attacks that exceed 1.5 tbps; it was the target of a record DDoS attack that flooded this web host at a rate of 620 gbps, where the reason for this attack was the default credentials, as mentioned in [11]. In Japan in May 2018, over 60 cameras nationwide were illegally accessed [12], and in most cases, a message that reads "i'm hacked. bye2" has been left on their screens by the hacker; the reason for this attack is the default passwords as a mentioned. In June 2017, F-secure discovered multiple vulnerabilities in Foscam-made IP cameras [13]. The vulnerabilities allow an attacker to remotely control a device and its video feed and download files from its built-in server. The attacker could access the network and its resources if an exploited device has access to a local network. An attacker could also use the device to perform other malicious activities, such as DDoS attacks against other parties. As mentioned in the above article, changing the default password is recommended; this is the best practice that should always follow. As mentioned above, the reasons for the above attacks are using default login credentials and poor security and privacy features. The motivation for an attacker could be violating privacy, access to video footage, access to the WVSS network, disabling video feeds, and performing DDoS attacks. Because WVSSs are employed in essential areas, only authorized agents should be able to monitor and manage them. Privacy and security are the primary issues while using such systems. Therefore, a mechanism is needed to detect the weakness of passwords for WVSS-IP cameras.

Existing password checker approaches are discussed. There are two basic approaches to calculating password strength. The first approach is based on the complexity of the password itself, such as calculating password strength as Shannon entropy [14] or employing statistical approaches [15]–[17]. The second approach is to simulate the adversary's password-guessing abilities, such as calculating password strength as the number of guesses required by an attacker to guess a given password [18]. Many studies have shown that the password-entropy measure is ineffective for measuring the strength of user-chosen passwords and is only suitable for assessing the strength of randomly generated passwords [19]. For user-created passwords, the entropy metric requires knowing the probability distribution of passwords. Accurate measurement of the password probability distribution requires a significant number of password samples [16]. Password checkers for password meters frequently utilize the password's "entropy" or "score" to estimate password strength, such as NIST password entropy [20]. This approach is also known as rule-based password-strength measures. Rule-based methods use various bonus and decrement rules to measure the password's "entropy." Password scores are often calculated by password length, the usage of digits, lowercase letters, uppercase letters, special characters in the password, and whether or not the password contains blocklisted words. The rule-based password measure algorithm zxcvbn [21] separates a given password into many patterns and then evaluates the entropy of each pattern separately. The following patterns are taken into account: repeat (e.g., 222, fff); sequence (e.g., 4567 and abcd); reversed (to reverse a word, e.g., drow); keyboard (e.g., qwerty). Suppose any of these weak patterns emerge in a given password. In that case, the algorithm only considers that specific part of the password to take it from a limited space of possibilities for calculating overall strength. The final password entropy is calculated as the sum of the entropy of each pattern. Password guessing, which examines the strength of a password from the standpoint of an attacker's abilities, is an approach that is similar to password strength estimation in many aspects. Password-guessing algorithms list the guesses in descending order of probability, which implies that the most common passwords are checked first, and a password guessed later is stronger. As a result, researchers frequently utilize the number of tries to determine password strength [18]. In [22], [23] designed a guess-number calculator for password-guessing algorithms to compute the number of guesses for a given password directly. It associates a password with the number of guesses necessary to guess the password. The guess-number calculator does not require running a guessing algorithm but can know the number of guesses for each password. For example, the guess-number calculator for the PCFG algorithm constructs a lookup table based on a training set and then computes the number of guesses for each password. This lookup table, however, is computationally slow to generate. tableAmico *et al.* [23] adopted an approximation method to calculate the number of guesses when employing n-gram models. Dell'Amico *et al.* [24] proposed a technique that does not need running a password-guessing algorithm to count the number of guesses for a given password. This technique utilizes fewer training data resources and has high convergence properties. Castelluccia *et al.* [25] proposed a password meter using Markov models. This method uses the Markov model to assign probabilities to each password, then uses the password's probability as the password strength. Melicher *et al.* [26] suggested a password-guessing attack technique based on an artificial neural network. The neural network may be reduced to several hundred kilobytes without significantly reducing password-guessing efficacy. similar to Markov models, neural networks in this technique are trained to produce the next character of a password given the previous characters. Cho *et al.* [27] proposed a HELPSE method to estimate the password's strength. It's a lightweight password strength estimation (LPSE) algorithm through a homomorphic encryption (HE) domain; this proposed method adopts numerical methods to perform the operations of the LPSE algorithm, which isn't provided in HE schemes. In addition, the LPSE algorithm is modified to increase the number of iterations of the numerical methods given depth constraints. Rule-based algorithms evaluate strength based on the password structure and some weak password patterns, and their accuracy is determined by their ability to capture the properties of user-chosen passwords. The current rule-based password-strength metric is insufficiently accurate due to the complexity of the users' password [28]. Password-guessing methods are thought to be the most accurate measurements of password strength [22], [24]. Still, they require prohibitive computing resources and a large amount of disk space, making them unsuitable for measuring password strength for password meters.

Regardless of these points, this paper develops and applies a fuzzy inference system (FIS) model based on IoT for checking the password strength in WVSS. The key benefits of the proposed approach are: i) this tool has a fast calculation speed to find an optimal solution, making it a suitable tool for real-time optimization of the password checker system, ii) unlike existing systems, the FIS-based approach optimizes the password characters to check the password's strength, and iii) unlike the existing systems, the proposed system detects the weak password and notifies the system administrator. The main idea of this paper is to apply the Mamdani FIS approach and evaluate its performance to optimize password characters to identify weak passwords.

2. PROPOSED IOT-FUZZY BASED PASSWORD CHECKER SYSTEM

In this IoT-fuzzy system, the Raspberry Pi chip was used as a controller, IP Camera, and two wireless antennas as transmitter/receiver devices. When the controller detects a weak password by checking the IP camera using the password checker algorithm, the algorithm will send an alert to the central system and cloud server that contains the warning from this IP camera node with the strength of the IP camera password as a percentage. This algorithm is applied to all IP cameras in the system.

The main aim of this system is to provide security and privacy for WVSS. The hardware module includes Raspberry Pi, IP camera, transmitter/receiver devices, hub device, and internet source. The block diagram of the proposed system is shown in Figure 2. IP camera and transmit device are connected to the Raspberry pi board directly through the hub device. Then the Raspberry Pi accessed the internet for the notification to be uploaded to the cloud server. Finally, the password checker algorithm detects weak passwords using the Mamdani FIS. Five password attributes (length, no lowercase, no uppercase, no digit, and no special character) will be relied on as input parameters of FIS, and the output parameter will be called the password strength ratio (PSR).

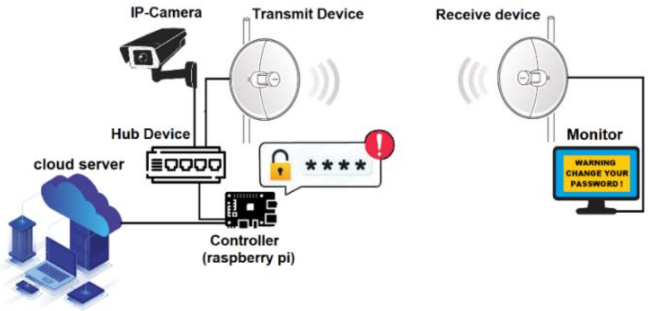


Figure 2. Block diagram of the proposed system

2.1. Password checker algorithm

The password checker algorithm using Mamdani FIS shown in Figure 3 consists of three steps: 1) password extraction and evaluate the input parameters stage, 2) processing stage (FIS), and 3) alarm stage. In the password extraction and evaluate the input parameters stage, five attributes are extracted from the IP camera's real-time streaming protocol (RTSP) link [29] using the counters. The RTSP is an application-level network communication system that transfers real-time data from multimedia to an endpoint device by communicating directly with the server streaming the data. This attribute was used as input parameters: length, no lowercase, no uppercase, no digit, and no special character. Firstly, the length is the sum of alphabets, digits, and symbols in the password. No lowercase is the sum of lowercase alphabets in the password. No uppercase is the sum of uppercase alphabets in the password. No digit is the sum of digits in the password. Finally, no special char is the number of symbols in the password.

Processing stage; the Mamdani FIS [30] was applied. The FIS includes three main components, fuzzification, rule base, and defuzzification, as shown in Figure 4. The fuzzification transforms the crisp value represented by the five input parameters into a degree of membership by using the corresponding membership functions. Rule base includes a set of linguistic statements called rules. These rules are in the form of IF antecedent, then consequence, where the antecedent consists of fuzzy input variables connected by logical functions (e.g., and, or, not), and the consequence is a fuzzy output variable called PSR. The defuzzification transforms the fuzzy output (PSR) into a crisp value that determines the password strength as a percentage. Finally, in the alarm stage. The algorithm will upload a notification with PSR of the IP camera to the cloud server and central system to alert the system administrator of this IP camera.

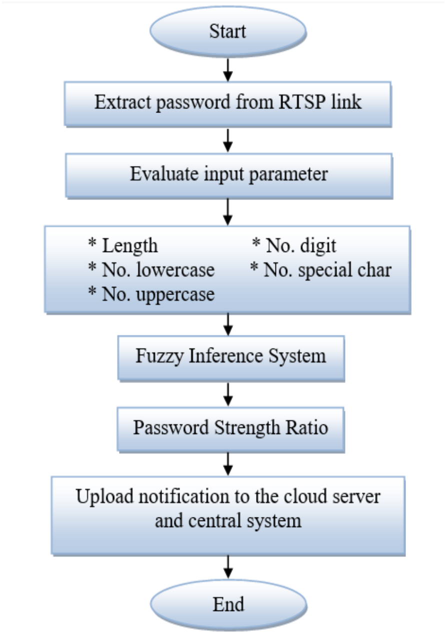


Figure 3. Flowchart of password checker algorithm

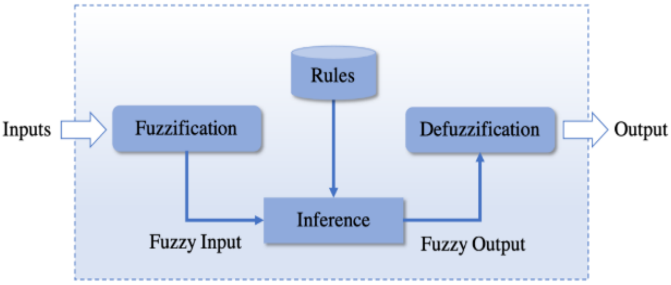


Figure 4. Fuzzy inference system

2.2. Password checker algorithm

The FIS is one of the most famous applications of fuzzy logic [31]. It can be helpful to achieve classification tasks, process control, online decision, and support tools.

2.2.1. Input membership functions design

Each input membership function is represented by a fuzzy set with two linguistic variables: weak and good. The equations of each input membership function for each linguistic variable are shown below, and its graphical representation is shown in Figure 5 for length, Figure 6 for no lowercase, Figure 7 for no uppercase, Figure 8 for no digit, and Figure 9 for no special char.

$$\mu\ \text{Length}_{\text{weak}} = \left\{ \begin{array}{cc} 1 & [0 - \ 7] \\ \frac{9-\text{Length}}{2} & [7 - \ 9] \end{array} \right\} \tag{1}$$

$$\mu\ \text{Length}_{\text{good}} = \left\{ \begin{array}{cc} \frac{\text{Length}-7}{2} & [7 - \ 9] \\ 1 & [9 - \ 100] \end{array} \right\} \tag{2}$$

$$\mu\ \text{No Lowercase}_{\text{weak}} = \frac{4-\text{No Lowercase}}{4} \quad [0 - \ 4] \tag{3}$$

$$\mu\ \text{No Lowercase}_{\text{good}} = \left\{ \begin{array}{cc} \text{No Lowercase} - & [4 - \ 100] \\ 1 & [4 - \ 100] \end{array} \right\} \tag{4}$$

$$\mu\ \text{No Uppercase}_{\text{weak}} = \frac{3-\text{No Uppercase}}{3} \quad [0 - \ 3] \tag{5}$$

$$\mu\ \text{No Uppercase}_{\text{good}} = \left\{ \begin{array}{cc} \frac{\text{No Uppercase}-3}{2} & [3 - \ 5] \\ 1 & [5 - \ 100] \end{array} \right\} \tag{6}$$

$$\mu\ \text{No Digit}_{\text{weak}} = \frac{2-\text{No Digit}}{2} \quad [0 - \ 2] \tag{7}$$

$$\mu\ \text{No Digit}_{\text{good}} = \left\{ \begin{array}{cc} \frac{\text{No Digit}-2}{3} & [2 - \ 5] \\ 1 & [5 - \ 100] \end{array} \right\} \tag{8}$$

$$\mu\ \text{No Special}_{\text{weak}} = 1 - \text{No Special} \quad [0 - \ 1] \tag{9}$$

$$\mu\ \text{No Special}_{\text{good}} = \left\{ \begin{array}{cc} \frac{\text{No Special}-1}{4} & [1 - \ 5] \\ 1 & [5 - \ 100] \end{array} \right\} \tag{10}$$

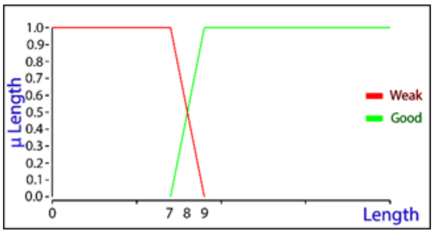


Figure 5. Length membership function

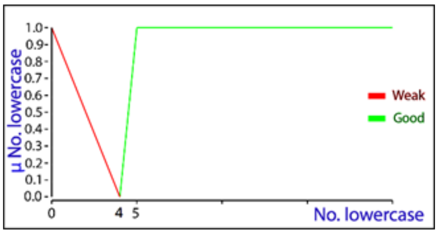


Figure 6. No lowercase membership function

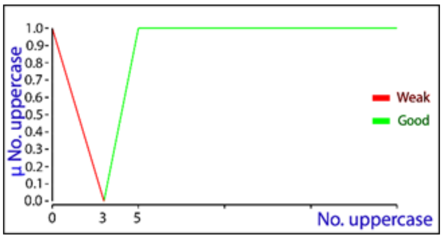


Figure 7. No uppercase membership function

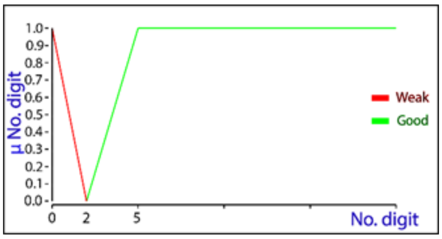


Figure 8. No digit membership function

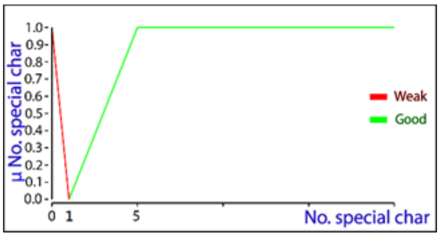


Figure 9. No special char membership function

2.2.2. Rule base design

The relationship between the inputs (length, no lowercase, no uppercase, no digit, and no special char) and the output variable (PSR) is performed through a collection of fuzzy rules. Every rule uses AND/OR connectors to associate various input factors with a specific output. The fuzzy rules for the password checker system are described in Table 1.

Table 1. Rule base of Mamdani FIS

Rules			Antecedents			Consequence
No	Length	No lowercase	No uppercase	No digit	No special	Psr
1	Weak	Weak	Weak	Weak	Weak	Bad password
2	Weak	Weak	Weak	Weak	Good	Bad password
3	Weak	Weak	Weak	Good	Weak	Bad password
4	Weak	Weak	Weak	Good	Good	Weak password
5	Weak	Weak	Good	Weak	Weak	Bad password
6	Weak	Weak	Good	Weak	Good	Weak password
7	Weak	Weak	Good	Good	Weak	Weak password
8	Weak	Weak	Good	Good	Good	Weak password
9	Weak	Good	Weak	Weak	Weak	Bad password
10	Weak	Good	Weak	Weak	Good	Weak password
11	Weak	Good	Weak	Good	Weak	Weak password
12	Weak	Good	Weak	Good	Good	Normal password
13	Weak	Good	Good	Weak	Weak	Weak password
14	Weak	Good	Good	Weak	Good	Normal password
15	Weak	Good	Good	Good	Weak	Normal password
16	Weak	Good	Good	Good	Good	Normal password
17	Good	Weak	Weak	Weak	Weak	Normal password
18	Good	Weak	Weak	Weak	Good	Normal password
19	Good	Weak	Weak	Good	Weak	Normal password
20	Good	Weak	Weak	Good	Good	Normal password
21	Good	Weak	Good	Weak	Weak	Normal password
22	Good	Weak	Good	Weak	Good	Strong password
23	Good	Weak	Good	Good	Weak	Strong password
24	Good	Weak	Good	Good	Good	Strong password
25	Good	Good	Weak	Weak	Weak	Normal password
26	Good	Good	Weak	Weak	Good	Strong password
27	Good	Good	Weak	Good	Weak	Strong password
28	Good	Good	Weak	Good	Good	Strong password
29	Good	Good	Good	Weak	Weak	Secure password
30	Good	Good	Good	Weak	Good	Secure password
31	Good	Good	Good	Good	Weak	Secure password
32	Good	Good	Good	Good	Good	Secure password

2.2.3. Output membership function design

PSR is the output membership function of the Mamdani FIS model. The PSR represents five linguistic variables (LV): bad password, weak password, normal password, strong password, and secure password. The range of each linguistic variable is shown in Table 2. The graphical representation of the triangle functions is shown in Figure 10.

Table 2. Output membership function of Mamdani model with range

LV	MF	Range	a	b	c
PSR	Bad password	[0,25]	-	0	25
	Weak password	[0,50]	0	25	50
	Normal password	[25,75]	25	50	75
	Strong password	[50,100]	50	75	100
	Secure password	[75,100]	75	100	-

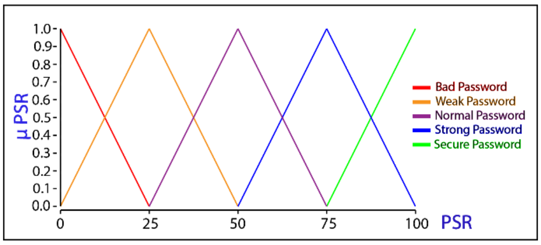


Figure 10. Output membership function of Mamdani FIS

The output of each rule is a fuzzy set derived from the output membership functions and the implication method of the FIS. The FIS's aggregation method aggregates these fuzzy output sets into a single fuzzy set. Then the combined output fuzzy set is defuzzified using the center of gravity (CoG) method as shown below to obtain the final crisp output value.

$$\mathrm{PSR} = \frac{\int \mu_{\mathrm{PSR}}.\mathrm{PSR}\ d\mathrm{PSR}}{\int \mu_{\mathrm{PSR}}\ d\mathrm{PSR}} \tag{11}$$

Where μ_{PSR} are the membership functions for output (PSR) of each linguistic variable, the result of (11) is the PSR (crisp value) as a percentage.

3. EXPERIMENTAL RESULTS

The experimental results in Table 3 are obtained after executing the password checker algorithm on WVSS, shown in Figure 11. The obtained results showed that the password checker algorithm had high accuracy in detecting weak passwords. The algorithm notified the system administrator with an alert to change the login password, as shown in Figure 12.

Table 3. Experimental results of PSR

Passwords	PSR (%)
Admin	8.333
Fliradmin	50.000
123456	8.333
Wbox123	50.0
Admin1234@#	74.999
ADMINfire12&$	90.277

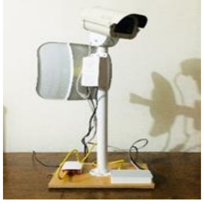
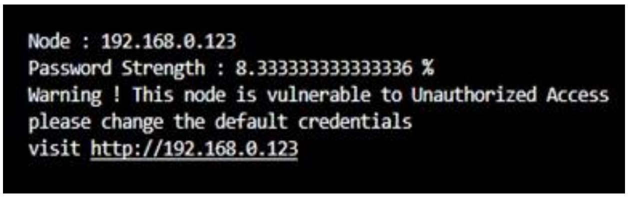


Figure 11. Hardware configuration for WVSS



```
Node : 192.168.0.123
Password Strength : 8.333333333333336 %
Warning ! This node is vulnerable to Unauthorized Access
please change the default credentials
visit http://192.168.0.123
```

Figure 12. Alert message for the system administrator

4. CONCLUSION

This work studies the vulnerability of a WVSS in the internet environment against unauthorized access by using weak passwords; a password checker algorithm was proposed to measure the strength of login credentials. The algorithm is based on the Mamdani FIS model and achieves much higher accuracy than commonly used password meters. Furthermore, the fine-grained measurement of the password strength provided by this algorithm allows for very precise feedback to the system administrator. The accuracy of this algorithm was evaluated by performing extensive experiments and showed that it outperforms existing schemes. In the future, an IoT-based fuzzy system will be upgraded to detect physical attacks on the WVSS and IoT devices.

ACKNOWLEDGEMENTS

Authors thanks the College of Engineering at the Iraqi University for providing the appropriate equipment and environment for experiments

REFERENCES

[1] N. Bari, G. Mani, and S. Berkovich, "Internet of things as a methodological concept," in *2013 Fourth International Conference on Computing for Geospatial Research and Application*, Jul. 2013, pp. 48–55, doi: 10.1109/COMGEO.2013.8.

[2] A. K. Triantafyllidis, C. Velardo, D. Salvi, S. A. Shah, V. G. Koutkias, and L. Tarassenko, "A survey of mobile phone sensing, self-reporting, and social sharing for pervasive healthcare," *IEEE Journal of Biomedical and Health Informatics*, vol. 21, no. 99, pp. 1–10, Jan. 2015, doi: 10.1109/JBHI.2015.2483902.

[3] M. Rai, A. Asim Husain, T. Maity, and R. Kumar Yadav, "Advance intelligent video surveillance system (AIVSS): A future aspect," in *Intelligent Video Surveillance*, IntechOpen, 2019.

[4] L. Ang, K. P. Seng, L. W. Chew, L. S. Yeong, and W. C. Chia, *Wireless multimedia sensor networks on reconfigurable hardware*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013.

[5] T. Zhang, A. Chowdhery, P. (Victor) Bahl, K. Jamieson, and S. Banerjee, "The design and implementation of a wireless video surveillance system," in *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, Sep. 2015, pp. 426–438, doi: 10.1145/2789168.2790123.

[6] J. Kim and N. Park, "Lightweight knowledge-based authentication model for intelligent closed circuit television in mobile personal computing," *Personal and Ubiquitous Computing*, vol. 26, no. 2, pp. 345–353, Apr. 2022, doi: 10.1007/s00779-019-01299-w.

[7] Y. Li, D. Han, and J. Yan, "Design and implementation of a wireless video surveillance system based on ARM," in *SPIE 8009, Third International Conference on Digital Image Processing (ICDIP 2011)*, Apr. 2011, p. 6, doi: 10.1117/12.896143.

[8] P. Vennam, P. T. C., T. B. M., Y.-G. Kim, and P. K. B. N., "Attacks and preventive measures on video surveillance systems: A review," *Applied Sciences*, vol. 11, no. 12, pp. 1–17, Jun. 2021, doi: 10.3390/app11125571.

[9] "Smart home device adoption reaches 36%, according to Parks Associates," *Parks Associates*, 2021. http://www.parksassociates.com/blog/article/pr-08172021 (accessed Jun. 27, 2022).

[10] L. Zhou, W. Q. Yan, Y. Shu, and J. Yu, "CVSS: A cloud-based visual surveillance system," *International Journal of Digital Crime and Forensics*, vol. 10, no. 1, pp. 79–91, Jan. 2018, doi: 10.4018/IJDCF.2018010107.

[11] J. Fruhlinger, "The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet," *CSO online*, 2018. https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html (accessed Jul. 03, 2022).

[12] "Dozens of canon security cameras hacked in Japan," *Kyodo News*, 2018. https://english.kyodonews.net/news/2018/05/91ec861ae24d-dozens-of-security-cameras-hacked-in-japan.html?phrase=ham fighters&words= (accessed Jul. 03, 2022).

[13] "Multiple flaws in Foscam IP cameras open devices, networks to attackers," *F-Secure*, 2017. https://www.f-secure.com/en/press/p/multiple-flaws-in-foscam-ip-cameras-open-devices-networks-to-attackers (accessed Jul. 03, 2022).

[14] J. Bonneau, C. Herley, P. C. V. Oorschot, and F. Stajano, "Passwords and the evolution of imperfect authentication," *Communications of the ACM*, vol. 58, no. 7, pp. 78–87, Jun. 2015, doi: 10.1145/2699390.

[15] M. Weir, S. Aggarwal, M. Collins, and H. Stern, "Testing metrics for password creation policies by attacking large sets of revealed passwords," in *Proceedings of the 17th ACM conference on Computer and communications security - CCS '10*, 2010, p. 162, doi: 10.1145/1866307.1866327.

[16] J. Bonneau, "The science of guessing: Analyzing an anonymized corpus of 70 million passwords," in *2012 IEEE Symposium on Security and Privacy*, May 2012, pp. 538–552, doi: 10.1109/SP.2012.49.

[17] J. Bonneau, "Statistical metrics for individual password strength," in *International Workshop on Security Protocols*, 2012, pp. 76–86, doi: 10.1007/978-3-642-35694-0_10.

[18] B. Ur *et al.*, "Measuring real-world accuracies and biases in modeling password guessability," in *24th USENIX Security Symposium*, 2015, pp. 463–481.

[19] S. Egelman, A. Sotirakopoulos, I. Muslukhov, K. Beznosov, and C. Herley, "Does my password go up to eleven?," in *CHI '13: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Apr. 2013, pp. 2379–2388, doi: 10.1145/2470654.2481329.

[20] W. E. Burr *et al.*, "Electronic Authentication Guideline," Gaithersburg, MD, Nov. 2013. doi: 10.6028/NIST.SP.800-63-2.

[21] D. L. Wheeler and D. Inc, "zxcvbn: Low-Budget Password Strength Estimation," in *Proceedings of the 25th USENIX Security Symposium*, 2016, pp. 157–173.

[22] P. G. Kelley *et al.*, "Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms," in *2012 IEEE Symposium on Security and Privacy*, May 2012, pp. 523–537, doi: 10.1109/SP.2012.38.

[23] M. Dell'Amico, P. Michiardi, and Y. Roudier, "Password Strength: An Empirical Analysis," in *2010 Proceedings IEEE INFOCOM*, Mar. 2010, pp. 1–9, doi: 10.1109/INFCOM.2010.5461951.

[24] M. D.'Amico and M. Filippone, "Monte carlo strength evaluation: Fast and Reliable Password Checking," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, Oct. 2015, pp. 158–169, doi: 10.1145/2810103.2813631.

[25] C. Castelluccia, M. Durmuth, and D. Perito, "Adaptive password-strength meters from Markov models," *NDSS*, 2012, pp. 1-14.

[26] W. Melicher *et al.*, "Fast, lean, and accurate: Modeling password guessability using neural networks," *25th USENIX Security Symposium (USENIX Security 16)*, 2016.

[27] M. Cho, K. Lee, and S. Kim, "HELPSE: Homomorphic encryption-based lightweight password strength estimation in a virtual keyboard system," in *Proceedings of the Great Lakes Symposium on VLSI 2022*, Jun. 2022, pp. 405–410, doi: 10.1145/3526241.3530338.

[28] X. D. C. D. Carnavalet and M. Mannan, "A large-scale evaluation of high-impact password strength meters," *ACM Transactions on Information and System Security*, vol. 18, no. 1, pp. 1–32, Jun. 2015, doi: 10.1145/2739044.

[29] I. Santos-González, A. Rivero-García, J. Molina-Gil, and P. Caballero-Gil, "Implementation and analysis of real-time streaming protocols," *Sensors*, vol. 17, no. 4, p. 846, Apr. 2017, doi: 10.3390/s17040846.

[30] M. F. Azeem, *Fuzzy inference system-theory and applications*. InTech, 2012.

[31] L. A. Zadeh, "Fuzzy sets," *Information and Control*, vol. 8, no. 3, pp. 338–353, Jun. 1965, doi: 10.1016/S0019-9958(65)90241-X.

BIOGRAPHIES OF AUTHORS

Mohammed Ahmed Jasim was born in Baghdad, Iraq, in1996. He received a B.Sc. degree in software engineering from Al Mansour University College, Baghdad, in 2017. He is currently studying M.Sc. in Computer Engineering at Al Iraqia University College of Engineering, Iraq. He can be contacted at email: mohammed.a.jasim@students.aliraqia.edu.iq.

Tayseer Salman Atia is a professor at the department of computer engineering, Al Iraqia University, Iraq, where she has been a faculty member since 2012. From 2013-2014 she was the head of the computer engineering department. From 2014-2015 she was the dean's assistant for scientific affairs. Tayseer graduated with a first-class B.Sc. degree in computer science in 2004 and an M.Sc. in data security in 2007 from the University of Technology, Iraq. She completed her Ph.D. in computer science from Al Mosul University, Iraq. Her research interests are data security and artificial intelligence, especially computational intelligence techniques. She can be contacted at email: tayseer.salman@aliraqia.edu.iq.