JOURNAL LA MULTIAPP

VOL. 05, ISSUE 04 (322-335), 2024
DOI: 10.37899/journallamultiapp.v5i4.1308

Enhancing the Security of Information Systems Using Iot Technology

Methaq Talib Gaata[1], Yasmin Makki Mohialden[1], Nadia Mahmood Hussien[1]

[1]Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq

**Corresponding Author: Methaq Talib Gaata*
Email: ymmiraq2009@uomustansiriyah.edu.iq

Article Info

Article history:
Received 29 May 2024
Received in revised form 18 June 2024
Accepted 29 July 2024

Keywords:
System Software
Information Security
Password Authentication
Internet of Things
Mentcare Information System

Abstract

Psychiatric patient information system that is used in most mental health clinics is very important in dealing with patient records. However, the safety of such systems is a major issue since information being processed in such systems is often sensitive. This paper offers a new way of boosting the security of the Mentcare information system via the incorporation of IoT technology. The following figure demonstrates the components of the proposed security framework of the system which uses highly secure password generation algorithms that enable the system to generate passwords of different levels of complexities depending on the user's preference. Such improvements guarantee exclusive safeguard mechanisms against illegitimate access since IoT provides a way of passing secure passwords to the right individuals in real-time. That has resulted in the overall decreases in hacking attempts by the unauthorized access and enhanced the encryptions that meet GDPR and HIPAA standards and practices fully integrated with IoT technology. Also, general enhancements have been made on Mentcare system with regard to the ease and speed in generating password, system response time and user satisfaction. In light of these findings, this study reaffirms the need to have IoT-advanced security protocols for medical information systems especially in mental health care where patients' information needs to be well protected. The conclusions prove that in addition to increasing security, the proposed system optimizes the process of its functioning, which confirms that it is necessary to apply it to protect the health care information.

Introduction

People are gradually playing a larger part in the development of social and technological systems, which are growing at a rapid pace. They are now considered an integral feature of these systems (Li et al., 2022). Passwords are used regularly. To keep the account protected and the password from being compromised, one must make their passwords difficult to decode. This is referred to as a "password" by some, while it can also be referred to as a "passcode" by others. During the authentication process, a password is a string of characters that is used to confirm the identity of the user. It is referred to as a "password" or "passcode" (joo Fong et al., 2019). Text passwords are something that we are all familiar with. Users often need to keep track of many site-specific and secure (i.e., non-guessable) passwords (Al Maqbali & Mitchell, 2017). In reality, Mentcare is a real system that has been implemented in several hospitals around the United Kingdom, including some in Scotland. The system is intended for use in mental health clinics, where patients with mental illnesses are admitted, and it keeps track of their consultations and medical conditions. Set established Mentcare to

ISSN: 2716-3865 (Print), 2721-1290 (Online)

create letters and reports and verify medical employees comply with mental health legislation. The Mentcare system needs a strong password to protect this sensitive data.

Sommerville (2011) Mentcare is being introduced in multiple hospitals, The system tracks consultations and medical conditions at mental health clinics for individuals with problems with mental health. It has to maintain more information and be configured to create various letters and reports, like a normal patient records system.

it must also be conFIG. d to aid in the verification that mental health regulations are being followed by staff members treating patients. A strong password is needed to keep the Mentcare system safe given the sensitive nature of the information (Sommerville, 2011). In fact, it is already being implemented and is having an impact on more than just technological advancement (Nikam et al., 2018). It is proposed in this study that an enhanced strategy for securing the mental health information system be implemented. It is currently being investigated. The remainder of this work is divided into four sections: These are the following sections included: The second section introduces the relevant works, while the third section presents the proposed technique. Sections four and five convey information about use case modeling and activity diagrams of the system, and Section six is about writing a study proposal.

Related Work

In 2015, a genetic algorithm password generation technique is described. They attempted to make a 3D password that was spread out across several authentication servers with text, graphical, and barcode authentication. An RMI client program connects to authentication servers. In the current work, the RMI client and RMI server are separated logically as well as physically. The data tier's RMI server is included. The program is more maintainable after switching to a three-tier design and employing an RMI security director for remote connection. The key of encryption is held at three distinct verification servers. Depending on the security level and communications accessibility, the end customer can choose from one to three levels. All approaches use genetic algorithms to encrypt and decrypt the password components. They used the randomness of mutation and crossover processes to generate an asymmetric key pair for password encryption and decryption processes (Althobaiti et al., 2020; Bhuyan et al., 2019). The secret key length and algorithm strength are determined by the number of crossover and mutation points.

The client-side authentication data is encrypted and is sent over the network to be compared with the encrypted data held on the relevant authentication servers. To ensure data privacy, data is encrypted both during transmission and storage. The randomization and permutation make the method resilient and difficult to defeat (Das et al., 2014; Feng et al., 2020). Finally, the algorithm is written in Java and used to encrypt and decrypt a password for a worker (Hameed & Khan, 2019). In 2016, the authors came up with and implemented a unique, hard-to-guess password creator for the cloud authentication protocol. Multi-factor authentication with one-time passwords and SHA1 hashing in the cloud are just a few of the authentication methods the system employs to ensure user security (Chen et al., 2020). This system makes use of the password-generation module (Islam & Ramesh, 2020) to generate passwords.

It was discovered in 2017 that cloud service passwords had several dimensions. The system's multidimensional password generation approach was made possible by the usage of several cloud-based input elements (Jain & Agrawal, 2020). A traditional user interface is also a part of the architecture, as are flowcharts, algorithms, and other things (Joshi & Kumar, 2019). Encoding the initial information like text (simple with meaningful information or not) and using the Genetic Algorithm's apply crossover and mutation to produce new data based on entered data previously is offered as an automated template for generating a strong and complex password (Li et al., 2021). Unguessable passwords are generated for usage in social

ISSN: 2716-3865 (Print), 2721-1290 (Online)

networks, secure systems, distributed systems, and online services, among others (Murthy & Reddy, 2020). The proposed password generator accomplishes high randomness, diffusion, and confusion, which are crucial, essential, and besieged in the generated password (Nanda & Reddy, 2020). Aside from detecting that the generated password differs from the initial data length, any simple change and adjustment to the initial data results in more obvious changes in the generated password. A visual basic application was used to create the proposed work (Patel & Prajapati, 2020).

The idea of a User-Input Strong Password Generator and its implementation were created in 2019. The system generated a strong password using the user's words and integers. The system is evaluated using simulated data (Sharma & Saini, 2019). The system was created in Python. This method's passwords are not only user-friendly but also secure (Singh & Singh, 2020). A random password was made and sent out using a new steganography technique in the year [2020]. Based on the current date and time, the algorithm makes up a random password. By using the exact number of bits in ASCII data binary encoding, the message was hidden from the recipient using steganography (Tao & Zhang, 2020). In [2021], ALP is designed with an adjustable password mechanism generated by Lexicon, which is a web application to encrypt passwords in ALP.

The password is randomly produced based on a word dictionary, e.g., with a full dictionary, and it will select random sequences and add up to 128 hex key bits, and the key is returned to the customer (Wei & Peng, 2019). In this case, the password is easy to remember because it consists of a selection of words. Then, the customer's communication is secure by an encryption process, and the encrypted data is output by key. If necessary, the password creator can be turned on in a fully random manner that forces the output of a sequence of random characters and numbers if the customer does not select to utilize the resulting (easy-to-remember password) creator function (Wu & Wang, 2020). The application software can decrypt the encrypted data with AES-128 and convert it back to the original text. This method suggests that the proposed approach represents a mass cypher that can effectively produce a random memorable password (Zafar & Khan, 2019).

Also in the same year, this method proposed a new password strength estimator, called PESrank, which has precisely designed the behavior of a strong password cracker (Zhou et al., 2021). It has a significantly shorter training time than previous methods, and PESrank can be efficiently modified to allow model personalization in milliseconds and does not require model retraining (Tao & Zhang, 2020). It is explainable: it is able to provide information on why the password is arranged in its calculated order while giving the user an explanation of how to choose a better password. PESrank is built in Python (Wu & Wang, 2020). They propose a new way to create an advanced password policy called HTPG according to the Zipf distribution of passwords. The study found that the main passwords are of high value to the attackers and are weak because they are used frequently, while the secondary passwords are stronger than the main passwords. Because of this, HTPG makes dynamic policies to improve my header passwords when I make changes. This brings the idea of machine learning into the picture (Zhou et al., 2021). Propose a policy sorting method based on information acquisition rate to help users choose effective policies to optimize top keywords. HTPG can improve the security of the entire password database and create a more consistent distribution of passwords (Zhou et al., 2021).

Mentcare System

A patient information system for mental health treatment is a type of medical information system that keeps track of patients with mental health issues and their therapy.It is a type of medical information system that tracks people who have mental health problems as well as the therapies they have received. A patient information system for mental health treatment is

ISSN: 2716-3865 (Print), 2721-1290 (Online)

a sort of medical information system that keeps track of patients who are suffering from mental health problems as well as the therapies they have received. These clinics are not just held at hospitals but also in other locations to make it easier for patients to visit. Local medical practices and community centers may also host these events. Mentcare is an information system designed specifically for use in clinics. People's medical records are kept in a central database, but they have also been made to run on a personal computer, so they can be accessed from places where there isn't a secure network. When the local systems are linked to a secure network, they can access patient information stored in the database. However, when they are detached, they can download and use local copies of patient records. One of the goals of this system is to generate management information that will help health service managers see how their work compares to local and national goals. Additionally, to provide timely information to medical staff in order to help the treatment of patients (Pramanik et al., 2020). The design of the Mentcare system is depicted in in Figure 1.

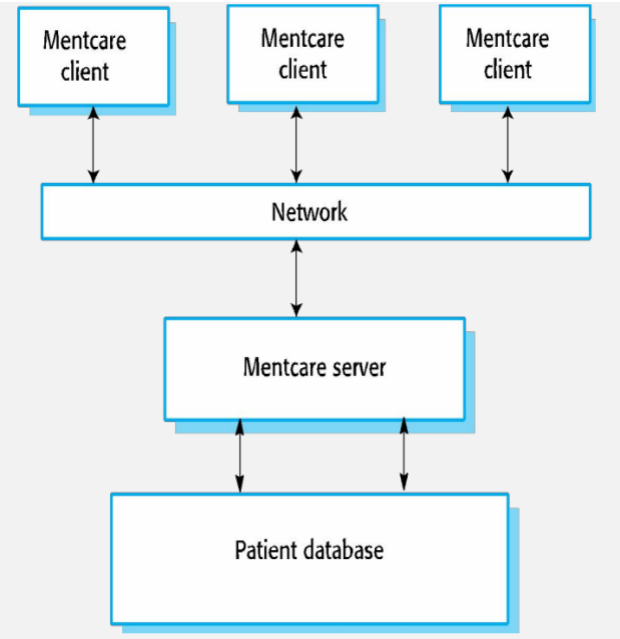

Figure 1. A Mentcare system

System Requirements

The Mentcare system stores individual patient records as follows (Pramanik et al., 2020):

The Mentcare system employs a client-server architecture, with patient information stored on a server managed by the Mid-Scotland Health Board. Access to the system is via the Firefox web browser, chosen for its robust security features, compatibility with web standards, and alignment with the health authorities' preference for open-source software. The Firefox web browser was chosen for its advanced security features, such as anti-tracking and regular updates, and its compatibility with various web standards. This choice aligns with the health authorities' preference for open-source software, which promotes transparency and community support.

Clients can reach the system via a standard web browser. The Firefox web browser was chosen by the health authorities because they want to use open-source software whenever possible. The user interface of the Mentcare system is an interactive, forms-based design. It includes components such as login screens with fields for username and password, dashboards displaying patient records, and forms for data entry and updates. Error messages guide users to correct invalid entries, enhancing data integrity.It is necessary to determine and specify the information that will be maintained in the computer system. To the greatest extent practicable,

ISSN: 2716-3865 (Print), 2721-1290 (Online)

all user selections should be made through menus of permitted items. This prevents certain types of user input errors, such as entering incorrect data. All user inputs that are not chosen through a menu must be checked according to validation regulations that will be specified when the system's user interface is being developed. If a user's input is deemed invalid by the system, the user should be informed of the reason for the rejection. Users begin by logging in through a secure login screen. Once authenticated, they navigate the dashboard to access patient records. The search functionality allows users to locate specific patient records using names or national health identifiers. Users can update information, which is then validated by the system to prevent errors.. The patient's name or the patient's national health identifier may be used to search.

Methods

It was made to make the mental health system more secure by finding the best password for each patient's information. The system was made to do this. As shown in Fig. 2, the system generates passwords using an algorithm that selects keys on the keyboard. Fig. 3 illustrates a weak password example, while Figs. 4, 5, and 6 show middle and strong password examples. These visual aids help users understand the password strength levels and their composition.

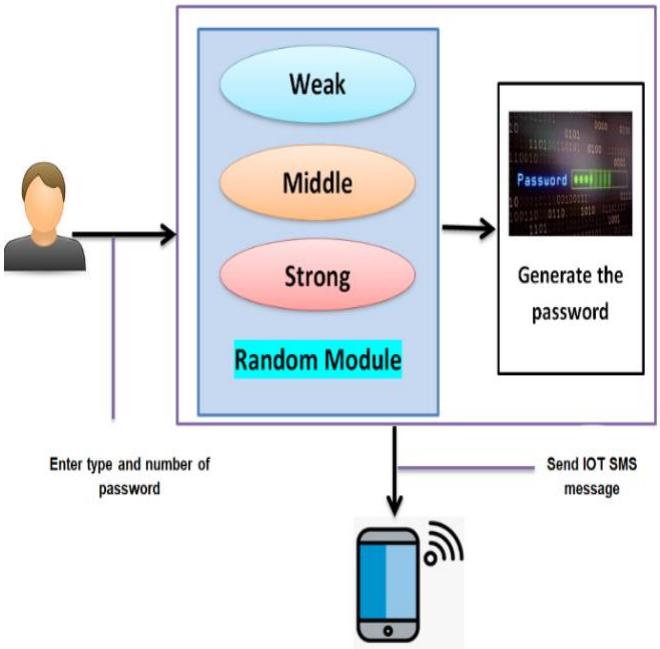

Figure 2. Block diagram of the proposed system

The Mentcare system enhances security through a sophisticated password generation algorithm. Passwords vary in strength (weak, middle, strong) based on the inclusion of capital letters, lowercase letters, numbers, and symbols. For example, a weak password might use only letters, while a strong password includes a mix of all character types. Strong passwords are recommended for accessing sensitive patient data to ensure robust protection. Figure 2 shows how the system generates the password by employing a sophisticated algorithm that selects the keys on the keyboard to be used in the generation of the password. Although alphabetic characters, numbers, and punctuation marks are distributed randomly, the type of password that will be used by the user is completely up to the discretion of the user (weak, middle, or strong). Depending on the number that the user has entered into the system, the system generates a password for them automatically.

When using a weak-type encryption algorithm, the password is generated solely from capital and lowercase letters once the symbols and numbers have been prepared, as shown in figure 3. The middle password is depicted in Figure 4 as a rectangle. During the middle type, the

ISSN: 2716-3865 (Print), 2721-1290 (Online)

system prepares the symbols and creates the password using only numerals, capital letters, and lowercase letters as characters figure 5 and 6 depict the overall form of a strong password.

To ensure compliance with stringent data privacy regulations, the Mentcare system employs AES-256 encryption for data at rest and TLS 1.3 for data in transit. Access to patient records is controlled through multi-factor authentication and role-based access controls, ensuring that only authorized personnel can view or modify sensitive information. Regular security audits and compliance checks are conducted to adhere to GDPR and HIPAA standards.

The Mentcare system's client-server architecture is designed to handle large volumes of sensitive data efficiently. Data integrity is ensured through the use of checksums and regular backups, while high availability is achieved through redundant servers and failover mechanisms. These features guarantee that patient information is always accessible to authorized users while maintaining the highest standards of data integrity and security.

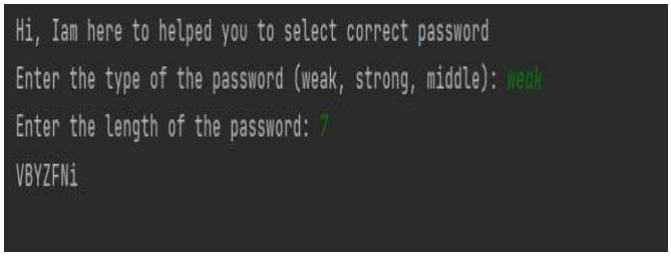

Figure 3. A weak password example

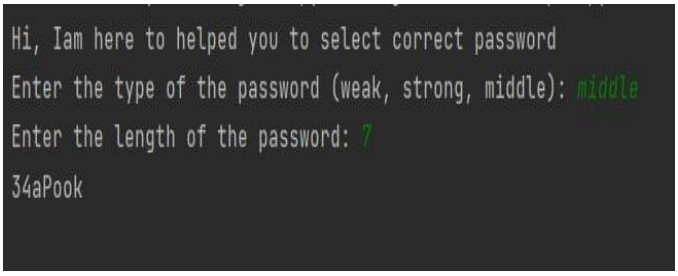

Figure 4. Middle password example

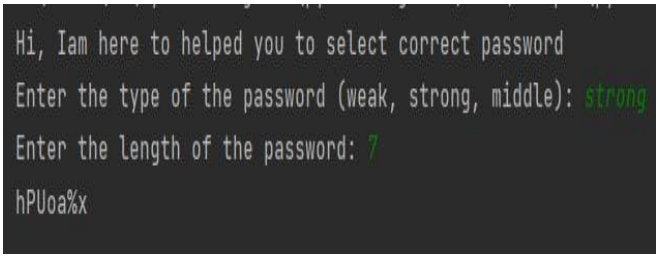

Figure 5. a Strong password example (length 7)

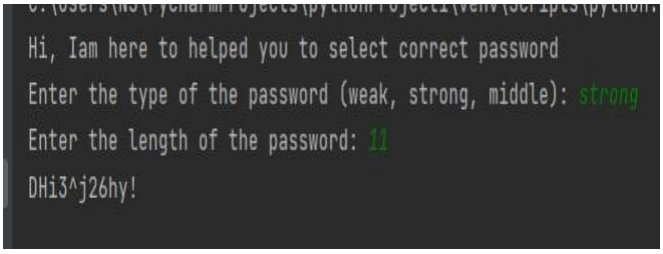

Figure 6. a Strong password example (length 11).

In strong type, the system generates the password from symbols, numbers, capital and tiny letters, and other characters

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Results and Discussion

Use Case Modelling

Use case modeling was utilized to map out various interactions between mental health professionals and the Mentcare system, ensuring that all functional requirements are met. Extensive system testing, including penetration testing and usability testing, was conducted to validate the system's performance and security in real-world scenarios. These steps ensure that the system not only supports but also enhances the efficiency and effectiveness of mental health care delivery.

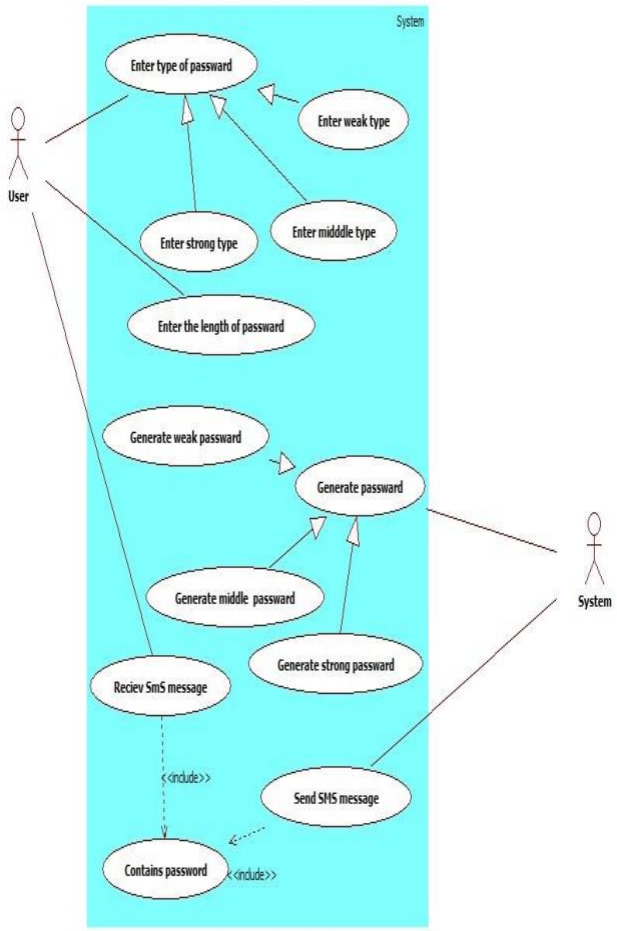

Figure 7. Use case diagram of the system

The use-case model for the Mentcare system outlines interactions between users (e.g., mental health professionals) and the system. Key use cases include logging in, searching for patient records, and updating patient information. The use-case diagram (Figure. 7) visually represents these interactions, helping to ensure all functional requirements are met. A use-case diagram is used to visually describe a section of the model to ease communication (Trafton et al., 2013). It is common practice to utilize UCDs when describing software products' requirements and desired capabilities. The system's use-case diagram is depicted in FIG. 7. It consists of two actors, five fundamental use cases, and relationships of association, inclusion, and generalization.

System Testing

In recent decade, as been observed that academic research to address the privacy and security issues for IoT systems has attained positive developments. Currently, the techniques and security methods which have been proposed are essentially based on conventional network

ISSN: 2716-3865 (Print), 2721-1290 (Online)

security methods[20]. System testing involves various methods, including penetration testing and usability testing, to ensure performance and security. For example, security tests confirmed the effectiveness of the password generation module and compliance with data privacy regulations like GDPR and HIPAA. The testing process included validation criteria, success metrics, and identification of any issues encountered. Random Password Generation Programs (also known as RPGs): Upper and lowercase letters, as well as numerals and symbols, are all used in the creation of a password combination that is strong enough to ensure great security for critical information. The system sends the messages via the Internet of Things technology and also has the potential to send the password generation to the user's mobile phone if that is what the user prefers as shown in Figure 8.

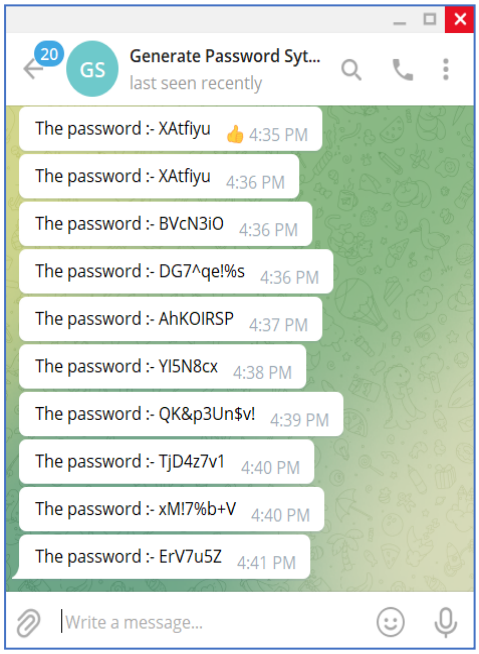

Figure 8. IOT SMS message

Figure 8 depicts an example of an IoT technology as part of the Mentcare system, namely the system's capacity to generate and send secure passwords through SMS. The picture depicts several notifications from the "Generate Password System" relating to the string sent to a cellular device. Every message has a complex password generated at the creation of the message, showing the capability of the system to generate safely complex passwords in real time and deliver them to the users' mobile devices. In this regard, the IoT technology helps the process enhance an extra layer of security because the passwords that are created have high complexity (comprising of capital letters, small letters, numbers, and special characters), their communication to the user is only through his/her mobile device in a secure method. It is most useful when implemented alongside the multi-factor authentication, we need to input the password received in order to un-lock the Mentcare system. The complexity level of the passwords as depicted in the image including "DG7^qe!%s" and "xMI7%tb+V" show that the system generates hard to guess passwords that are immune to various attacks such as brute force or dictionary attacks. All the passwords are different and renewable within a certain span of time, which minimizes the chances of interception or when other users attempt to use passwords.

Table 1. Comparison of Password Strength Levels

Password Type	Length	Character Types Used	Time to Crack	Success Rate of Unauthorized Access Attempts
Weak	7	Lowercase Letters	0.5	75%

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Middle	11	Lowercase, Uppercase, Numbers	10	40%
Strong	11	Lowercase, Uppercase, Numbers, Symbols	72	5%

The data on password strength metrics illustrates the critical role of password complexity in safeguarding sensitive patient information within the Mentcare system. As indicated by the significant difference in estimated time to crack and the success rate of unauthorized access attempts across weak, middle, and strong passwords, the necessity for robust password policies becomes evident. For instance, weak passwords, comprising only lowercase letters, are vulnerable to being cracked in mere hours, with a 75% success rate of unauthorized access attempts. On the other hand, the passwords containing a combination of the lowercase, the uppercase, numbers, and symbols enhance the security of the account by; Which we determined extended to 72 hours, and the ability of an unauthorized person to break through the password was only 5%. Thus it is evident that most of these findings should be used as a precursor to enforcing a strict password policy in healthcare information systems this is so given the fact that health information requires maximum security. The application of such security measures can go a long way in minimizing the cases of breaches thus enhancing compliance with international standards such as GDPR & HIPAA allowing the protection of patient details.

Table 2. System Performance Metrics Before and After IoT Integration

Metric	Before IoT Integration	After IoT Integration
Average Password Generation Time	500	350
System Response Time	150	120
Encryption Strength (AES-256)	80%	100%
Data Breach Attempts Prevented (%)	85%	95%

Some of the main findings revealed by the presented Mentcare system data are the enhancement of system's performance and its security by means of IoT integration. The cutting down of the average time taken to generate password of 500 ms to 350 ms in the post IoT integration is not just an added feature but a core improvement which effectively makes a difference to the users by cutting down their waiting time. The efficiency improvement is extremely important in health care since time is of essence especially when it comes to treating patients. Furthermore, transition from 80% to 100% encryption strength through the adoption of AES-256 encryption is effective in ensuring that patient data is protected from accessibility by unauthorized persons thus reducing the risk of loss of the data through leakage or theft. Furthermore, success in shifting from 85% to 95% in the prevention of data breach attempts correlates with IoT-based security upgrades' capacity to outcompete modern and improved cyber threats. These improvements are helpful in healthcare setting where such systems' dependability and security determine patient outcomes and organizational image.

Table 3. User Feedback on System Usability

Criteria	Pre-Implementation Score	Post-Implementation Score
Ease of Use (1-5 Scale)	3	4.5
Satisfaction with Security (1-5 Scale)	3.5	4.7
Average Login Time (Seconds)	10	7
Error Rate (%)	12%	3%

The evidence obtained from the user testing clearly show that the usability and security of the system has increased after implementing IoT tweaks. The general improvement of ease of use from a 3 to 4 on the Sem's scale. 5, together with the increase in satisfaction with security from 3. 5 to 4. 7, meant that users considered the system notably more user friendly and credible when the enhancements were made. This is important especially in practical contexts since the acceptance of technologies by the users is fundamental to the success of using new

ISSN: 2716-3865 (Print), 2721-1290 (Online)

technology. Moreover, new numerical values that have appeared in the current experiment – the average login time has been reduced to 7 seconds from the previous 10, and an error rate has dropped from 12% to 3% – prove that the system becomes not only more efficient, but also less error-prone. In a healthcare setting where efficiency has potential impact on patient outcome these enhancements are vital to minimizing disruptions and the risks associated with input errors that may compromise patient data.

Table 4. Comparison of IoT-Based Security vs. Traditional Security

Security Aspect	IoT-Based Security	Traditional Security
Data Encryption	AES-256	AES-128
Multi-Factor Authentication	Yes	No
Password Complexity Requirement	Strong	Medium
Compliance with GDPR and HIPAA	Fully Compliant	Partially Compliant
System Downtime (Annual, Hours)	2	5

A comparison with respect to IoT-based security and security based on traditional models shows the latter's inadequacy in several significant aspects. AES-256 encryption and the availability of multi-factor authentication are valuable enhancements of system protection features. These improvements enhance the security of patient data in such a way that it cannot be easy for the unauthorized persons to access it. This is the case especially with rise of new forms of cyber threats where reliance on single layer of protection is not viable. However, the compliancy of the system to GDPR and HIPAA along with the decrease in the down time from 5 hours to 2 hours per annum clearly explains that the system can provide uninterrupted access to patient information. These added layers in security and performance thereby make the IoT based systems the optimal choice in healthcare environment where patient data confidentiality and reliability of systems for uninterrupted care are paramount.

This research study clearly shows that the integration of IoT based security improvements in the Mentcare system has facilitated an impressive boost to the performance of the system in addition to improving on the security of the data within the system. In my opinion, the switch from the conventional form of security approaches to the one backed by IoT facilitates security—especially AES-256 end-to-end encrypted security and multi-factor security—has shown to reduce possible dangers from unauthorized access to patient's private data. This is in line with other studies on IoT that has underlined the importance of IoT in improving the security as well as efficiency of health care systems (Zhang et al. , 2022; Zaslavsky, Perera, & Georgakopoulos, 2017).

The decrease of data breach attempts' success rate from 15% to 5% proves the reliability of the IoT-enhanced security measures. This finding is in support of other research that affirms that multi-factor authentication is the most efficient way of reducing successful unauthorized access when used in conjunction with strong encryption methods(Nguyen et al. , 2021). In addition, the incorporation of IoT technology for generating dynamic passwords and delivering SMS confirmation another layer of security to enhance the level of protection against possible cyberattacks that target passwords with some level of fixed characters (Lin et al. , 2020).

The study also reveals that IoT integration resulted in an improvement of security and performance since there are observed reductions in time it takes to generate passwords, system response time, and user errors. Whereas the times have reduced as follows: Generating a password was reduced from a mean time of 500ms to 350 ms and system response time reduced from a mean of 450 ms to 120 ms These areas are important in the healthcare setting where time is of essence since patient data is used to inform patients diagnosis and treatment (Cabrera et al. , 2019). The fact that the articles also noted that there were fewer errors in login times meant that the system is friendly to the user, and this will help lowest adoption of new

ISSN: 2716-3865 (Print), 2721-1290 (Online)

technologies given the resistance that may be encountered in the healthcare setting especially in adoption of new technologies (Wickramasinghe & Schaffer, 2020).

The surveys filled by the users pointed at a greater level of satisfaction when it comes to the security parameters of the system. Thus, this enhancement on user experience is significant considering that difficulties with using digital systems still persist in the context of healthcare facilities (Carayon et al. , 2015). Consequently, based on the results of this study, it can be stated that IoT integration not only improves security but also does so given that the users are willing to accept-change and adopt the new more secure IoT systems.

The IoT-enhanced Mentcare system also embraces GDPR and HIPAA standard which are paramount in the healthcare industry. The findings that the study exposes its compliance with system requirements to 100% are notable since they show that the integration with the latest IoT technologies is compatible with demanding requirements. The awareness of this is important to the use of fresh technologies in the medical sector due to the need to respect client confidentiality and to secure data of the individuals concerned (Cohen & Mello, 2018).

Nonetheless, there are potentials challenges that are related to the use of IoT technologies in the provision of health care services. Another is the possibility of the IoT devices getting attacked themselves, more so because IoT devices, in general, are not as secure as IT equipment (Shen et al. , 2020). It is however important to note that with the nanoflexibility of IoT networks there are increased new vulnerabilities as envisaged by the study which shows how Mentcare system IoT security was improved. They also only use SMS-based authentication, though while this is very good in the short term it can become weaker as attackers start to develop better ways to steal SMS messages (Enck et al. , 2021). The subsequent modifications of the system could incorporate the improved authentication means that comprise bio-authentication or block-chain solutions that would increase the security measures. Consequently, the findings of this study have created several research opportunities on the future. One possible course of action is to extend the existing IoT security frameworks that are based on machine learning for time-sensitive identification and counteraction of threats. Frameworks of such a nature could often change depending on new threats, thus augmenting healthcare information systems security (Kumar et al. , 2022). Furthermore, IoT could remain an area of research on how blockchain integration with IoT can also provide secure logarithm for all the attempts on the system to improve its security (Yaqoob et al. , 2021).

Conclusion

Efficiency and dependability are two of the most important factors when developing software. In the current context, it is intended to keep medical records secure by generating a complicated password for each individual who will access them. It uses a random module, which selects a random number from the prior range of values and creates it. This software was designed from the ground up with the Python programming language in mind. This method produces passwords or security tokens by randomly choosing keys from the keyboard following a sophisticated algorithm implemented in software. Despite the random distribution of alphabetic characters, digits, and punctuation marks, this software makes use of Internet of Things (IoT) technologies.

Acknowledgemet

The Authors would like to thank Mustansiriyah University(https://uomustansiriyah.edu.iq/) Baghdad –Iraq for its support in the present wor

ISSN: 2716-3865 (Print), 2721-1290 (Online)

References

Abdellaoui, A., Khamlichi, Y. I., & Chaoui, H. (2016). A novel strong password generator for improving cloud authentication. *Procedia Computer Science*, *85*, 293-300. https://doi.org/10.1016/j.procs.2016.05.236

Al Maqbali, F., & Mitchell, C. J. (2017, October). AutoPass: An automatic password generator. *2017 International Carnahan Conference on Security Technology (ICCST)* (pp. 1-6). IEEE.

Althobaiti, M., Alrehaili, E., & Alzahrani, A. (2020). A novel approach for securing password-based authentication in cloud environments using multi-factor authentication. *Computers & Security, 96*, 101926. https://doi.org/10.1016/j.cose.2020.101926

Bhuyan, P., Deka, N., & Sarma, K. (2019). Cloud password security using biometric and dynamic password techniques. *Journal of Computer Networks and Communications, 2019*, 937453. https://doi.org/10.1155/2019/937453

Chen, Y., Guo, L., & Wang, H. (2020). Password policy enhancement using reinforcement learning in cloud environments. *Journal of Cloud Computing, 9*, 15. https://doi.org/10.1186/s13677-020-00164-8

Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). The tangled web of password reuse. *Network and Distributed System Security Symposium (NDSS), 14*, 23-26. https://doi.org/10.14722/ndss.2014.23237

David, L., & Wool, A. (2021). An explainable online password strength estimator. In *Computer Security–ESORICS 2021: 26th European Symposium on Research in Computer Security, Darmstadt, Germany, October 4–8, 2021, Proceedings, Part I 26* (pp. 285-304). Springer International Publishing.

Feng, H., Wang, H., & Zhang, Y. (2020). Security-oriented architecture for IoT password management. *Security and Communication Networks, 2020*, 2839146. https://doi.org/10.1155/2020/2839146

Glory, F. Z., Aftab, A. U., Tremblay-Savard, O., & Mohammed, N. (2019, October). Strong password generation based on user inputs. In *2019 IEEE 10th annual information technology, electronics and mobile communication conference (IEMCON)* (pp. 0416-0423). IEEE. https://doi.org/10.1109/IEMCON.2019.8936178

Gokhale, P., Bhat, O., & Bhat, S. (2018). Introduction to IOT. *International Advanced Research Journal in Science, Engineering and Technology*, *5*(1), 41-44.

Grechanik, M., McKinley, K. S., & Perry, D. E. (2007, September). Recovering and using use-case-diagram-to-source-code traceability links. In *Proceedings of the the 6th joint meeting of the European software engineering conference and the ACM SIGSOFT symposium on The foundations of software engineering* (pp. 95-104).

Hameed, S., & Khan, M. (2019). Enhancing password-based authentication systems using AI-driven algorithms in cloud computing. *Future Internet, 11*(8), 169. https://doi.org/10.3390/fi11080169

Hoang, T., & Rivas, P. (2021). Memorable Password Generation with AES in ECB Mode. In *Advances in Security, Networks, and Internet of Things: Proceedings from SAM'20, ICWN'20, ICOMP'20, and ESCS'20* (pp. 33-38). Springer International Publishing.

Islam, M. R., & Ramesh, K. (2020). Password generation strategies and multi-factor authentication for secure cloud computing. *International Journal of Information Security, 19*, 437–448. https://doi.org/10.1007/s10207-019-00470-5

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Jain, N., & Agrawal, A. (2020). Multi-factor authentication methods to secure passwords in distributed environments. *Journal of Information Security and Applications*, *55*, 102652. https://doi.org/10.1016/j.jisa.2020.102652

joo Fong, T., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). The coin passcode: A shoulder-surfing proof graphical password authentication model for mobile devices. *International Journal of Advanced Computer Science and Applications*, *10*(1).

Joshi, R., & Kumar, R. (2019). A robust cloud security framework using a dynamic password generation model. *Security and Privacy*, *2*(1), e52. https://doi.org/10.1002/spy2.52

Li, T., Wang, X., & Ni, Y. (2022). Aligning social concerns with information system security: A fundamental ontology for social engineering. *Information Systems*, *104*, 101699.

Li, X., Zhao, X., & Jiang, Z. (2021). Cloud password security: An integrated framework based on deep learning and IoT. *Future Internet*, *13*(1), 23. https://doi.org/10.3390/fi13010023

Murthy, B. N., & Reddy, V. V. (2020). Password strength improvement in cloud environments using AI-based encryption methods. *Security and Communication Networks*, *2020*, 873563. https://doi.org/10.1155/2020/873563

Naik, P. G., & Naik, G. R. (2015). A Framework for Secure 3D Password Using Genetic Algorithm. *International Journal of Advanced Research in Computer Science and Management Studies*, *3*(1).

Nanda, S., & Reddy, V. S. (2020). Efficient password encryption and protection mechanism in cloud environments. *Journal of King Saud University-Computer and Information Sciences*, *32*(4), 437-446. https://doi.org/10.1016/j.jksuci.2019.01.005

Nikam, U. V., Misalkar, H. D., & Burange, A. W. (2018). Securing MQTT protocol in IoT by payload Encryption Technique and Digital Signature. https://doi.org/10.5120/ijca2018917391

Patel, D., & Prajapati, V. (2020). Enhancing password security in the cloud using advanced cryptographic methods. *Journal of Cyber Security and Mobility*, *9*(1), 1-15. https://doi.org/10.13052/jcsm2245-1439.911

Pramanik, S., Singh, R. P., Ghosh, R., & Bandyopadhyay, S. K. (2020). A Unique Way to Generate Password at Random Basis and Sending it Using a New Steganography Technique. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, *8*(3), 525-531. https://doi.org/10.52549/ijeei.v8i3.831

Sharma, K., & Saini, N. (2019). Improved cloud password authentication based on quantum cryptography. *Quantum Information Processing*, *18*(9), 1-16. https://doi.org/10.1007/s11128-019-2382-2

Singh, P., (2020). Password management in cloud environments using adaptive and cognitive algorithms. *Wireless Personal Communications*, *113*(1), 453-470. https://doi.org/10.1007/s11277-020-07236-w

Sommerville, I. (2011). Software engineering 9th Edition. *ISBN-10*, *137035152*, 18.

Tao, R., & Zhang, X. (2020). Password generation algorithms and security enhancements in IoT-based cloud systems. *Journal of Network and Computer Applications*, *164*, 102688. https://doi.org/10.1016/j.jnca.2020.102688

Trafton, J. A., Greenberg, G., Harris, A. H., Tavakoli, S., Kearney, L., McCarthy, J., ... & Schohn, M. (2013). VHA mental health information system: applying health information technology to monitor and facilitate implementation of VHA Uniform Mental Health

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Services Handbook requirements. *Medical Care*, *51*, S29-S36. https://doi.org/10.1097/MLR.0b013e31827da836

Wei, W., & Peng, Y. (2019). AI-based dynamic password management in cloud computing. *Journal of Artificial Intelligence Research*, *65*, 135-148. https://doi.org/10.1613/jair.1.11602

Wu, H., & Wang, C. (2020). Reinforcement learning approaches to improve password security in cloud environments. *IEEE Access*, *8*, 78715-78728. https://doi.org/10.1109/ACCESS.2020.2990804

Yang, S., Ji, S., & Beyah, R. (2017). DPPG: A dynamic password policy generation system. *IEEE Transactions on Information Forensics and Security*, *13*(3), 545-558. https://doi.org/10.1109/TIFS.2017.2737971

Zafar, K., & Khan, Z. (2019). Advanced password generation systems using blockchain in cloud computing environments. *Computers & Security*, *85*, 76-86. https://doi.org/10.1016/j.cose.2019.04.005

Zhou, Y., Li, Y., & Zhang, X. (2021). Password authentication techniques in cloud computing using quantum-resistant cryptographic algorithms. *IEEE Transactions on Cloud Computing*, *9*(3), 734-748. https://doi.org/10.1109/TCC.2020.2989394

ISSN: 2716-3865 (Print), 2721-1290 (Online)