User Authentication System for Securing and Identifies by User and IoT Device

B. Bamleshwar Rao[1], Dr. Akhilesh A. Waoo[2]

{bamleshwar@gmail.com[1], akhileshwaoo@gmail.com[2]}

AKSU, Satna[1], AKSU, Satna[2]

Abstract. The primary goal of Secured IoT is to safeguard IoT data from a wide range of security threats and attacks. Data encryption is challenging to implement because of the restricted nature of the Internet of Things devices. the vast majority of users should be able to access IoT data without difficulty. Authenticating IoT people rather than the devices they use is becoming increasingly widespread in the Internet of Things (IoT) security solutions. An understandable fear for patients' safety arises when unauthorized access to data and devices is allowed in the healthcare setting. Transmitting data safely requires that the parties involved maintain the confidentiality of the data they are exchanging. For the protection of Internet of Things data, we proposed using a Lightweight Block Cipher based on a Substitution and Permutation Network (SPN). A block cipher for Internet of Things data security based on the Feistel structure has been created. To protect the information coming from the Internet of Things, develop a hybrid algorithm for generating one-time-use passwords.

Keywords: Substitution and Permutation Network, One Time Password (OTP), internet of things (IoT), User Authentication, Security in Healthcare.

1 Introduction

When a new piece of technology is introduced, security is always the most pressing concern that needs to be addressed right away. Devices connected to the Internet of Things are being used to collect a large quantity of information on people, and this is especially true in the IoT ecosystem, where this information is being collected at an alarming rate. Because the Internet of Things is still in its infancy and connects a varied range of communication technologies, security is a significant concern for many people. As the popularity of this technology develops, so does the number of hackers who target it, necessitating the adoption of a higher level of protection from the start of the process. There is around one million more Internet of Things devices likely to be deployed in a range of application domains around the world each year, according to current estimates. As the number of interconnected devices continues to expand at an exponential rate, security weaknesses are becoming increasingly frequent, increasing the likelihood of a cyberattack occurring. Therefore, fraudsters will have more opportunities to exploit vulnerabilities in these domains as a result of the increased importance placed on their security. After 2020, it is anticipated that investment in Internet of Things

THEETAS 2022, April 16-17, Jabalpur, India

DOI 10.4108/eai.16-4-2022.2318076

security would expand at a higher rate. Because of these and other circumstances, the requirement for security in an IoT environment is heightened, as is the need for security in a context where devices and networks have limited resources available.

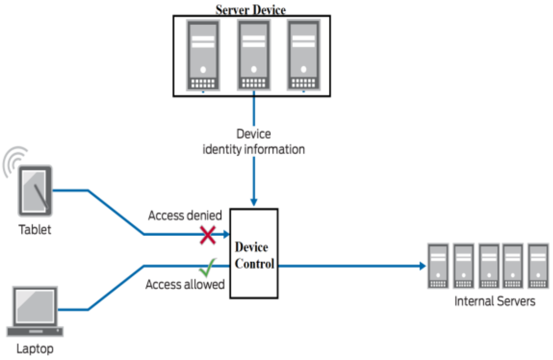

Fig. 1. Authentication System That Identifies by User and Device.

As a result, current security solutions were ill-suited for use with the Internet of Things, which was a consequence of this. A detailed explanation of why more sophisticated security measures are required is provided in the next section:

- The Internet of Things (IoT) devices are designed to operate on low-speed Central Processing Units (CPUs) and to be powered by rechargeable batteries. There is less space available for traditional encryption algorithms that involve complex calculations as a result of this reduction in available space. Defined as having a restricted memory capacity, Internet of Things devices are frequently constrained in their memory capacities. There is currently no security scheme that is designed specifically for devices with limited memory capacity.

- Interfacing with low data rate radio interfaces: Internet of Things devices have grown accustomed to connecting through low data rate radio interfaces. Using standard security procedures on Internet of Things-based systems is difficult due to the low bandwidth communication channels that are employed in these systems.

- Internet of Things operating systems that are too lightweight: Because the Internet of Things devices are deployed with a lightweight operating system, it is not viable to implement security fixes on IoT devices that are too lightweight. Aside from that, the lightweight Internet of Things operating system is lacking in components for accepting and incorporating new applications or libraries.

- It is possible for a mobile Internet of Things device that moves often to join or leave a network with no prior configuration or notification. Due to the inherent structure of network topologies, the performance of existing security solutions is adversely affected. As a result of this, the Internet of Things will be less likely to take advantage of these technologies.

- In the Internet of Things (IoT), heterogeneity is a given because it encompasses a broad range of wireless protocols such as WiFi, Zigbee, and Z-Wave as well as a diverse range of devices ranging from personal computers to RFID tags. As a result of the heterogeneous combination of diverse devices, it is difficult to implement efficient security solutions expediently.

2 Related works

R. Miller, et al[1] A session's authorization and confidence level can be defined by system administrators, allowing them to differentiate between a legitimate employee, a hostile employee within a corporation, and an intruder from outside the company. It is possible to develop virtual reality applications that require real-time behavioral verification of users to provide secure access to content using our technology.

Y. Gu et al.,[2] This research are being done to develop a behavior characterization technique that is specifically suited to prototype networks, to make it easier to extract domain-independent behavioral features while also making it possible to identify a new user in a new environment in a single step. According to a wide number of studies, WiONE beats its state-of-the-art competitors in terms of authentication performance while requiring significantly less training.

L. Lu et al., et al[3] Create a balanced binary tree-based authentication protocol that reliably recognizes every individual, to better identify each individual, by combining these binary classifiers and spoofer detectors only with the information provided by registered users.

D. Wang et al[4] Develop a better solution than the Truong et al approach for overcoming the obstacles that have been found while yet retaining reasonable efficiency. Identify and investigate the fundamental causes of the issues that have been highlighted.

Y. Ashibani et al[5] Tests on the proposed model were conducted using two datasets, and the results revealed that it is effective in authenticating users with the best accuracy, as indicated by low false positive, false negative, and equal error rates, among many other characteristics.

L. dos Santos Dourado et al[6] It is proved in this proof of concept that the semantic base (ontology) of a link is complex, but that the connection discovered in the photos is simple, and that as a consequence of this, the authentication system's robustness is shown as well

L. Chen et al[7] A new feature extraction method are employed to collect user behavior features from data, and then fusion technology is used to identify the users who have exhibited such characteristics. In this research, we can identify whether or not the current user is a normal human based on the outcomes of the recognition process.

3 Proposed methodologies

The performance and security issues that have arisen because of the rapid expansion of the Internet of Things must be resolved as soon as possible to ensure that the Internet of Things continues to grow at its current rate in the future. It is difficult to recover from problems that develop as a result of the Internet of Things (IoT), which harms the adoption of this technology. As part of the process of bringing the Internet of Things to life, standardization will be one of the most difficult obstacles to overcome. Other considerations include energy efficiency and security, as well as heterogeneity and interoperability, to name a few topics. Every one of these considerations must be taken into consideration by the Internet of Things (IoT) devices that are now being developed on an individual basis. As improved cryptographic algorithms have been developed over the past few years, it has become increasingly difficult to rely on old cryptographic procedures to safeguard sensitive information. To be effective against security vulnerabilities such as Brute Force or Eavesdropping attacks, any security algorithm must possess the following characteristics: active S-boxes with the least amount of Gate equivalent (if possible), a reliable permutation layer, low power dissipation, and the ability to deal with data complexity of the highest possible level. To achieve its important goal of identifying solutions for problems that arise when data is used in Internet of Things applications and infrastructures, one of the most significant objectives of this research is to identify problems that arise when data is used in the Internet of Things applications and infrastructures.

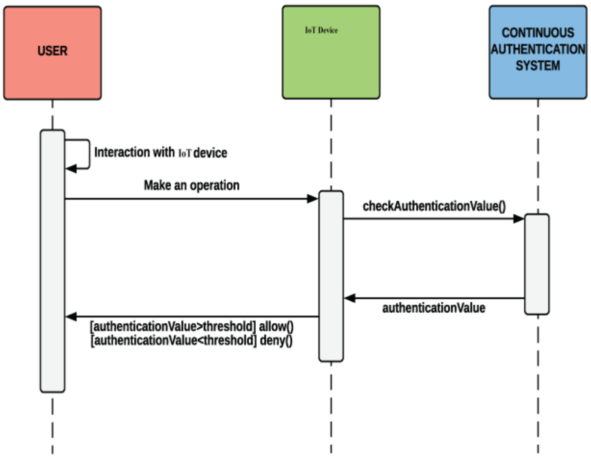
USER
IoT Device
CONTINUOUS AUTHENTICATION SYSTEM
Interaction with IoT device
Make an operation
checkAuthenticationValue()
authenticationValue
[authenticationValue>threshold] allow()
[authenticationValue<threshold] deny()

Fig. 2. IoT Device Communication.

The identification of solutions to the problems that arise when data is used in Internet of Things applications and infrastructures is another important goal of this research, which is also an important goal of this research. This research is also important because it is essential to the success of the Internet of Things. We want to uncover who we are as individuals, and that is one of the most significant aims of our research. One of the most important goals and purposes of the research is to identify and address the obstacles and challenges that have been identified. This is one of the most important goals and purposes of the research. With this inquiry, we hope to deconstruct and analyze the security requirements of secrecy and authentication in greater depth than has previously been done, allowing us to obtain a deeper knowledge of these requirements as a whole. Maintaining the perspective that data is being transmitted between two different locations is critical when developing symmetric lightweight algorithms for use in data security applications. As well as other sorts of assaults, this research will educate how to successfully battle differential, linear, algebraic, and other types of assaults, among other things. Before the authentication method can begin, authentication must take place between the user and the medical equipment to verify that the authenticity of both parties is validated. Once it has been determined that the verification process was successful, the technique moves on to the authentication portion of the operation. Once an authentication attempt has failed due to the patient or medical device failing to authenticate, the login request is forwarded to the registration procedure and a warning of authentication failure is given to the patient or medical device as a result of either the patient or the medical device's failure to authenticate. The authentication mechanism is initiated in the background when a successful login attempt has been completed. Both the patient and the medical gadget must be examined separately, and this is crucial. With the proposed approach, data security in the healthcare Internet of Things system is predicted to be improved, which is likely to benefit both patients and healthcare professionals. Three strategies are implemented by the organization to ensure that medical data is collected and applied safely. These are: The following are the most important components, according to those who have proposed the technique thus far: The use of SSL technology ensures that the registration of stakeholders in the smart healthcare system is a safe and secure process for all parties involved in the process. For the system to function correctly, it is necessary for everyone who is involved to be aware of the secret password. Ongoing research and development are focused on the creation of lightweight block ciphers for the protection of medical data against hostile hackers. Users can be confident that their information is delivered safely thanks to the use of a unique and secure key to transport data to the framework's user. It is only necessary to use a password once during the process to complete it successfully. Connections between things, products, and devices are being made to the internet to produce a smarter life that is fueled by the data that is being collected. Because it connects a vast number of products and people, and because it has the power of transporting data across the internet, it surpasses the limitations of traditional human-to-human and human-to-computer communication. There are several risks and challenges related to managing the large volumes of data generated by the Internet of Things (IoT) as the IoT ecosystem expands its reach as it grows in popularity. During data transmission, it is critical to consider the amount of processing power, the amount of energy consumed, and the amount of time spent encrypting and decrypting data before and after transmission. There is a growing demand for the integration of appropriate cryptographic solutions into embedded devices for the Internet of Things applications as a result of these developments. As a result of their low processing power, short battery life, tiny physical size, restricted memory, and absence of a power supply, embedded devices are severely limited in their ability to do calculations in the aggregate. Complicated cryptographic algorithms such as RSA, which necessitate a large key size and several sophisticated operations, cannot be implemented in these devices to overcome this limitation. The hardware footprints of algorithms must, however, be taken into mind when developing a security algorithm for resource-constrained devices. To solve all of the issues stated above, this research presents a state-of-the-art, lightweight cryptographic block cipher, SHA224 Jo, that can be used in the Healthcare Internet of Things environment to protect patient data. Because of the invention of computers and the development of the internet, new avenues for connecting everything and everyone at any time have been created. It raises worries about the security of the information that is being gathered and delivered by these devices when they are not linked securely to the network. Attackers or intruders are motivated to take advantage of weak or susceptible networks, putting the security of the information at risk. An advanced security algorithm is required to overcome such difficulties and prevent unauthorized users from having access to sensitive information about another individual. Even though there are several security algorithms available to authenticate remote users based on traditional passwords, biometrics, and other factors with varying efficiencies, the One Time Password (OTP) algorithm is more efficient in providing complete protection of the login-time authentication to the remote users. Some of its disadvantages include a high calculation cost, delayed delivery of the one-time password (OTP), memory consumption, safe computation of the one-time password, and vulnerability to security threats including impersonation and eavesdropping. Improvements in authentication methods that take into consideration the variety of Internet of Things devices and communication networks are therefore necessary. Consequently, in this research, a new hybrid OTP generating technique for safe access to IoT medical data from the CMS is proposed. This technique has been discussed in further detail elsewhere.

3.1 Proposed Algorithm

Input: The device's EPC / IMEI / IP / Mobile Number, the time stamp t, the counter value c, and the message m are all included. Process: The hybrid algorithm is used to generate the OTP.

Output: An OTP is used to authenticate the user's device.

```
    Step 1: Start
    Step 2: It is the medical gadget itself that saves the authentication information in the System.
    Step 3: The information included in a medical gadget is preserved in System.
    Step 4: Access to System data is requested by a user who requests authorization to do so.
    Step 5: After creating an OTP using the cryptographic block cipher, SHA224 algorithms, the System transfers the generated OTP over to the User device for verification.
    Step 6: The user resubmits the OTP to the system and requests the requested data.
    Step 7: If the OTP matches, the user is granted access to information.
    Step 8: Stop
```

The government considers cyber-security to be a major concern. proposed a suggested OTP methodology, is one method of eavesdropping since it employs a timestamp to generate a new secret value for each session of every data request that originates from the same user, even if that user makes the request more than once. Another advantage of the Lagrange interpolation is that it makes only tiny changes in the secret key with each repeat, which is a significant advantage. Consequently, even if an attacker or intruder manages to obtain access to the secret key or any other personally identifiable information about the user, that information will become worthless over time as a result of this constraint. To prevent replay attacks, a message authentication code (MAC) generates a new random number for each time the message authentication code is delivered. Additionally, the message authentication code includes a timestamp or nonce to identify when the message authentication code was sent. Observe in the image above that the former OTP is not being used in the construction of the new OTP in the proposed, as can be seen in the image above. It is less likely that a replay attack will take place as a result of these measures. It is also resilient to impersonation attempts as a result of the algorithm's successful defense against the replay attack, which makes it difficult to replicate. Masquerade and forgery attacks: If an intruder obtains hold of the users' credentials and attempts to gain access to the system using these user names, it is highly unlikely that the intruder will be able to generate the correct OTP because the algorithm uses the timestamp as a primary input to generate the OTP. Phishing attacks: If an intruder obtains hold of the users' credentials and attempts to gain access to the system using these user names, Phishing attacks: If an attacker obtains hold of the users' credentials and attempts to gain access to the system by using these user names, the system is considered compromised. The most essential security aspect of the proposed hybrid OTP generating algorithm, proposed security is that it generates OTP that is nearly completely random and unique for each trail, which is extremely crucial for trail security. As a result, it is impervious to fabrication and concealed assassination attempts.

3.2 Results Analysis

This hybrid OTP generating technique, which is illustrated in Table 1, is built in python and google colab using the configuration shown in the following screenshot. When multiple requests from a single user are verified in succession, an OTP is generated. This is achieved through the usage of python multi-threading functionality. Using the python multi-threading concept, this is made possible to achieve. This method has been tried and tested on both a desktop computer and an Android it has been confirmed to be effective. It is possible to connect two separate sets of connectors when utilizing the experimental configuration. There are two approaches to communicating with each other: Submission of a different number of OTP generation requests is essential to ascertain the length of time required for the server to calculate and interact to produce OTP. Failure to do so will result in the generation of incorrect OTP. To perform implementation using intel core i7 CPU@2.20 GHz, 8GB RAM, Window 10 operating system, Android 11.0, Anaconda Based python language The python application that generates the OTP is depicted in Figure 2 as it is being executed. For example, the RSA, ECC, SHA224, MD5 with other hash functions encryption algorithms, as well as the proposed encryption method, are utilized in this application to generate the secret key and to determine the amount of time it takes to generate the key. The key K is used to produce a one-time password (OTP) for each session, which is unique to that session. To evaluate the proposed hybrid OTP algorithm proposed, its specific qualities are compared to the specific properties of the other currently known OTP methods, and a table is constructed to show the differences between the two algorithms.

Table 1: Comparison of the Error rate of proposed algorithm and RSA, ECC, SHA224, MD5 with other hash functions with other OTP Algorithms.

Algorithm	**ECC**	**SHA224**	**Proposed**
Features			
Key Size	**512**	**512**	**256**
Computation Cost	**High**	**High**	**Low**
OTP requirements	**High**	**High**	**Low**

A comparative study of the proposed algorithm with other OTP algorithms concerning its resistance to various attacks is made and presented. Comparison of Attack Resistance of the proposed algorithm with other OTP Algorithms. Comparing the calculating time of the proposed algorithm to that of other OTP methods is one way to gauge its effectiveness. Using the hybrid OTP approach.

Performance of the proposed Algorithm on Different Devices.

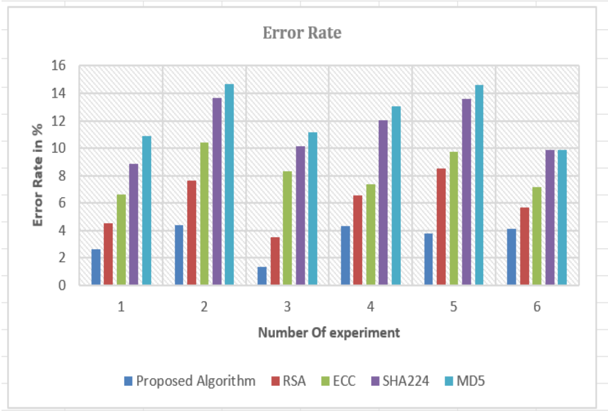

Fig. 3. Comparison of the Error rate of proposed algorithm and RSA, ECC, SHA224, MD5 with other hash functions.

4 Conclusions

This research work covers the security requirements for the Internet of Things in this research piece (IoT). The qualities of confidentiality, integrity, authentication, authorization, non-repudiation, availability, and privacy are all included in these standards. In addition, this examines and debates a wide range of literature from both the academic and corporate worlds. Each study is thoroughly analyzed to have a better understanding of the challenges and issues associated with data security in healthcare IoT systems. The results of an investigation into current research efforts are summarised, and the reasons for the investigation are described in more depth. According to the findings of the aforementioned literature analysis, data security in the healthcare business will be a major problem when the Internet of Things (IoT) becomes a reality. Other types of cryptographic attacks, such as differential, linear, differential linear, and algebraic assaults, are also covered in great detail by this writer. For the Internet of Things, secure communications are essential; yet, the security algorithms employed in the environment must be efficient enough for low-resource smart devices to work. The proposed algorithms should be able to boost the security of IoT data without sacrificing its integrity because of their reduced block and key sizes, as well as their simpler rounding. Measures including reduced memory and power consumption, as well as faster throughput, should be considered while evaluating the implementation efficiency of the proposed algorithms.

References

[1]R. Miller, A. Ajit, N. Kholgade Banerjee, and S. Banerjee, "Realtime Behavior-Based Continual Authentication of Users in Virtual Reality Environments," 2019 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR), 2019, pp. 253-2531, DOI: 10.1109/AIVR46125.2019.00058.

[2]Y. Gu et al., "WiONE: One-Shot Learning for Environment-Robust Device-Free User Authentication via Commodity Wi-Fi in Man-Machine System," in IEEE Transactions on Computational Social Systems, vol. 8, no. 3, pp. 630-642, June 2021, DOI: 10.1109/TCSS.2021.3056654.

[3]L. Lu et al., "Lip Reading-Based User Authentication Through Acoustic Sensing on Smartphones," in IEEE/ACM Transactions on Networking, vol. 27, no. 1, pp. 447-460, Feb. 2019, DOI: 10.1109/TNET.2019.2891733.

[4]D. Wang, H. Cheng, D. He, and P. Wang, "On the Challenges in Designing Identity-Based Privacy-Preserving Authentication Schemes for Mobile Devices," in IEEE Systems Journal, vol. 12, no. 1, pp. 916-925, March 2018, DOI: 10.1109/JSYST.2016.2585681.

[5]Y. Ashibani and Q. H. Mahmoud, "A Multi-Feature User Authentication Model Based on Mobile App Interactions," in IEEE Access, vol. 8, pp. 96322-96339, 2020, DOI: 10.1109/ACCESS.2020.2996233.

[6]L. dos Santos Dourado and E. Ishikawa, "Graphical Semantic Authentication," 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), 2020, pp. 1-6, DOI: 10.23919/CISTI49556.2020.9140446.

[7]L. Chen, Y. Zhong, W. Ai, and D. Zhang, "Continuous Authentication Based on User Interaction Behavior," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), 2019, pp. 1-6, DOI: 10.1109/ISDFS.2019.8757539.

[8]R. F. Olanrewaju, B. U. I. Khan, M. A. Morshidi, F. Anwar and M. L. B. M. Kiah, "A Frictionless and Secure User Authentication in Web-Based Premium Applications," in IEEE Access, vol. 9, pp. 129240-129255, 2021, DOI: 10.1109/ACCESS.2021.3110310.

[9]K. Riesen, T. Hanne and R. Schmidt, "Sketch-Based User Authentication With a Novel String Edit Distance Model," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 48, no. 3, pp. 460-472, March 2018, DOI: 10.1109/TSMC.2016.2601074.

[10]T. Zhu et al., "RiskCog: Unobtrusive Real-Time User Authentication on Mobile Devices in the Wild," in IEEE Transactions on Mobile Computing, vol. 19, no. 2, pp. 466-483, 1 Feb. 2020, DOI: 10.1109/TMC.2019.2892440.

[11]J. Tsai and N. Lo, "A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services," in IEEE Systems Journal, vol. 9, no. 3, pp. 805-815, Sept. 2015, DOI: 10.1109/JSYST.2014.2322973.

[12]B. Motella, M. Nicola and S. Damy, "Enhanced GNSS Authentication Based on the Joint CHIMERA/OSNMA Scheme," in IEEE Access, vol. 9, pp. 121570-121582, 2021, DOI: 10.1109/ACCESS.2021.3107871.

[13]Y. Gu et al., "WiONE: One-Shot Learning for Environment-Robust Device-Free User Authentication via Commodity Wi-Fi in Man-Machine System," in IEEE Transactions on Computational Social Systems, vol. 8, no. 3, pp. 630-642, June 2021, DOI: 10.1109/TCSS.2021.3056654.

[14]L. Lu et al., "Lip Reading-Based User Authentication Through Acoustic Sensing on Smartphones," in IEEE/ACM Transactions on Networking, vol. 27, no. 1, pp. 447-460, Feb. 2019, DOI: 10.1109/TNET.2019.2891733..

[15]K. Lee, C. Esposito and S. Lee, "Vulnerability Analysis Challenges of the Mouse Data Based on Machine Learning for Image-Based User Authentication," in IEEE Access, vol. 7, pp. 177241-177253, 2019, DOI: 10.1109/ACCESS.2019.2956819.

[16]K. M. Renuka, S. Kumari, D. Zhao, and L. Li, "Design of a Secure Password-Based Authentication Scheme for M2M Networks in IoT Enabled Cyber-Physical Systems," in IEEE Access, vol. 7, pp. 51014-51027, 2019, DOI: 10.1109/ACCESS.2019.2908499.

[17]M. T. Arafin and G. Qu, "Memristors for Secret Sharing-Based Lightweight Authentication," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 26, no. 12, pp. 2671-2683, Dec. 2018, DOI: 10.1109/TVLSI.2018.2823714.

[18]J. Zhou, Z. Cao, Z. Qin, X. Dong, and K. Ren, "LPPA: Lightweight Privacy-Preserving Authentication From Efficient Multi-Key Secure Outsourced Computation for Location-Based Services in VANETs," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 420-434, 2020, DOI: 10.1109/TIFS.2019.2923156.