A New Approach to Mitigating Authentication Challenge for an Internet of Things Paradigm

Adekunle A. Adeyelu
Benue State University
Makurdi, Nigeria

Oyeyemi E. Elusakin
Benue State University
Makurdi, Nigeria

Samera Uga-Otor
Benue State University
Makurdi, Nigeria

Ijeoma Rufina Godwin
Benue State University
Makurdi, Nigeria

Zakka Shirley John
Benue State University
Makurdi, Nigeria

ABSTRACT

The field of Internet of Things (IoT) has transpired as a field of incredible growth, impact and potential. Its technological advancement has led to the development of smart environments in which heterogeneous smart devices enable shared communication among one another. User authentication is one of the significant factors in the IoT environment as it allows the users to communicate with the devices securely. Integration of authentication technologies with IoT ensures secure data retrieval and robust access control. as the devices send and receive highly sensitive data for different purposes. If an attacker manages to steal or spoof biometric data, they could potentially bypass this factor. This study suggests another approach to securing a system through authentication. The new approach was an adaptation of the three factor (3FA) authentication technique introducing a graphical password alongside the traditional requirements. The algorithm was validated using Burrows, Abadi and Needham (BAN) logic. An informal security analysis was also conducted to verify the authenticity of this system. The algorithm is implemented using the Hypertext pre-Processor (PHP) programming language to build the user application interface for the control of the IoT devices. The implementation of this improved 3FA technique demonstrate highly improved security features when compared to other relevant security schemes

General Terms

User authentication, Internet

Keywords

Internet of Things, smart devices, authentication, 3FA, BAN logic, heterogeneous.

1. INTRODUCTION

The convergence of interconnected devices in the Internet of Things (IoT) forms a dynamic network driven by wireless sensor integration, facilitating a realm of intelligent services [1]. These devices, remotely manage and monitored, execute diverse functions autonomously. Within this interconnected web, their interactions transcend conventional communication paradigms, introducing a landscape where machine-to-machine communication supersedes traditional human-to-human and human-to-machine interactions [2]. This evolution not only redefines connectivity but reshapes the very fabric of interaction in our digital ecosystem.

The expansive landscape of the Internet of Things (IoT) heralds a realm brimming with potential, marked by exponential growth and far-reaching influence. This evolution converges diverse smart devices empowered by RFID, mobile capabilities, cloud computing, wireless connectivity, and sensor technologies, enabling seamless communication amongst them. The synergy among these technologies births an array of intelligent applications, ranging from the personalized domains of smart homes and e-health to the broader spectrum of smart city innovations [2]. The pervasive significance of IoT devices is unmistakable, evident in their seamless integration into our daily routines, notably in streamlining home automation tasks. Projections indicate a substantial surge in their adoption on the horizon. This heightened interest stems from multiple factors, notably the burgeoning consumer demand and a surge in inventive applications, prompting an amplified focus from both academic and industrial spheres [3]. The proliferation of IoT gadgets is on an upward trajectory, fueled by the simultaneous advancement of technology enabling internet connectivity for a myriad of physical objects. This exponential growth forecasts a substantial increase in internet-connected devices across various sectors such as healthcare, manufacturing, electrical processing, agriculture, and security [2]. However, this surge in connectivity has led to an unprecedented deluge of data, presenting both opportunities and challenges. While innovative business models and technological advancements have propelled IoT expansion, security and privacy concerns have risen alarmingly. Despite the transformative potential, insufficient attention to these concerns poses significant risks [3].

Security breaches in the IoT landscape demand urgent attention, particularly regarding the transmission and storage of sensitive user data. Current authentication methods like three-factor authentication (3FA) have been adopted but remain vulnerable to sophisticated attacks such as man-in-the-middle (MitM) attacks, compromising device security and granting unauthorized access. The pressing need for an enhanced 3FA system capable of thwarting MitM attacks within IoT environments is evident. Existing 3FA systems fall short in adequately safeguarding against such cyber threats, leaving IoT devices vulnerable to exploitation. Developing an upgraded 3FA system that not only elevates security levels but also effectively mitigates MitM attacks is paramount. This imperative endeavor aims to fortify IoT device security, significantly reducing the looming risks of cyber-attacks and ensuring the integrity of IoT ecosystems.

2. LITERATURE REVIEW

A taxonomy and literature review of IoT authentication with key considerations for developing authentication schemes in IoT networks and applications, particularly in sensor-based

applications were first highlighted by a group of authors. They emphasized the need for lightweight protocols that efficiently utilize minimal resources due to the constraints faced by sensors in terms of memory, processing power, and battery life [3]. These protocols should be easily implementable in such constrained environments. Moreover, the researchers highlighted the critical aspect of assessing the robustness of authentication techniques against a range of potential attacks. This includes evaluating their resilience against various threats like Sybil attacks, node capture, replay attacks, password guessing, message forging, brute force attacks, man-in-the-middle attacks, denial-of-service attacks, collision attacks, chosen-plaintext attacks, and more. Understanding and analyzing how these authentication methods fare against such threats are crucial aspects of designing secure IoT authentication protocols.

Another approach was presented as a robust three-factor remote user authentication protocol tailored for future IoT Wireless Sensor Network (WSN) applications. This protocol facilitated access for authorized remote users by enabling mutual authentication between the user and the IoT sensor node via a reliable gateway node. Upon successful mutual authentication, a symmetric session key (SK) was generated for ensuring secure future communications [4]. The protocol's security framework was grounded on the well-established BAN (Burrows-Abadi-Needham) logic, a widely recognized and accepted rationale for security protocols. Informal security assessments demonstrated the protocol's effectiveness in repelling common attacks. Furthermore, a formal security evaluation using the AVISPA simulation corroborated the protocol's security, affirming its capability to withstand potential threats and ensuring a robust authentication mechanism for IoT WSN applications. Further advances proposed a privacy-preserving authentication system called "PrivHome" aiming to uphold data confidentiality within smart home environments [5]. However, their protocols, reliant on symmetric key cryptosystems, encountered computational inefficiencies particularly concerning smart devices with limited resources. Consequently, their protocol faced challenges in maintaining the confidentiality of authentication parameters, highlighting limitations in effectively ensuring data security within such constrained IoT device settings. Another attempt was the introduction of a technique leveraging on public-key cryptography to establish and authenticate session keys within a smart home network. While showcasing the protocol's ability to resist various types of attacks, their approach exhibited several security vulnerabilities. Notably, weaknesses such as susceptibility to known-key attacks and device compromise were identified. Moreover, the protocol lacked assurances regarding secrecy and anonymity, both critical security aspects essential in the context of the Internet of Things [6]. A little work has been done on how to make the multiple-party user authentication method better. Elliptic curve cryptography (ECC)-based biometric-based two-party user authentication was proposed in 2020 [7]. In order to assure security and user anonymity, they proposed an improved hash-based two-party user authentication method for the client-server context. In another approach, a cutting-edge three-party user authentication method that enables two users to verify one another through a reliable third party was created [8]. A contribution to advancing authentication systems was proposed as an improved mechanism which was rigorously evaluated through the AVISPA simulation program [9]. Building upon previous works, they addressed the limitations observed in earlier efforts that couldn't withstand user impersonation attacks facilitated by stolen smart cards. Their solution introduced a lightweight authentication mechanism tailored for IoT systems. However, it's noteworthy that their method lacked the capability to ensure user anonymity, primarily due to overlooking known session-specific transitory information attacks, leaving a potential vulnerability in their approach. Moon et al [10] proposed a biometric-based authentication scheme to improve on security in IoT having been able to successfully prove that an adversary can impersonate a legitimate user or sensor node. They were also able to reveal the failure of previous works in carrying out illegal smart card revocation/reissue. They proposed an approach to address some of these challenges, which was able to strengthen the security of IoT. However, their scheme could only solve the weaknesses of impersonation attack amongst other security flaws. Fakroon et al. [11], proposed a new scheme for user authentication that combines physical context awareness and transaction history. The new scheme offers two advantages: it does not maintain a verification table and avoids clock synchronization problem. Communication overhead and computational cost of this scheme were lower compared with other related schemes. However, it was only able to mitigate to some extent man-in-the-middle attack and secure login and password change phase. In an attempt to address some of the critical security issues prevalent in an IoT-based network in a holistic manner, Saqib et al [12] proposed a lightweight three-factor authentication framework for IoT-based critical applications. This framework relied on elliptical curve cryptography and hash chains to achieve a signature-based 3-factor authentication system suitable for IoT. It is characterised by mutual authentication of the Gateway node with both the remote user and the sensor node, as well as the generation of dynamic session keys. This was accomplished between the nodes using a publish-subscribe pattern to prevent the induction of shadow IoT devices or rogue devices into the network. The proposed framework saved bandwidth and communication energy while reducing the computing and communication costs of resource-constrained sensor nodes but failed to determine the of the IoT devices as well as ensuring resistance to stolen mobile device attack.

3. METHODOLOGY

The multi-factor authentication (MFA) model which was widely used in various security systems and applications was adapted. It involves provision of an additional authentication parameter in what the user knows in addition to the traditional username, password, Personal Identity Number (PIN) and One Time Password (OTP) authentication of a user. In this system, the user is prompted to provide three or more of these factors in order to gain access to a protected resource by requiring a graphical user password in addition to the traditional provision of the user’s password, PIN, OTP or a specific gesture in order to gain access. The introduction of graphical password will make it more difficult for an unauthorized person to gain access to the account, even if they have the password and one-time code sent to the mobile phone. This approach strengthens the protection around the resource apart from the usual user's fingerprint or signature protection. Figure 1 shows the different stages of authentication of the proposed scheme.

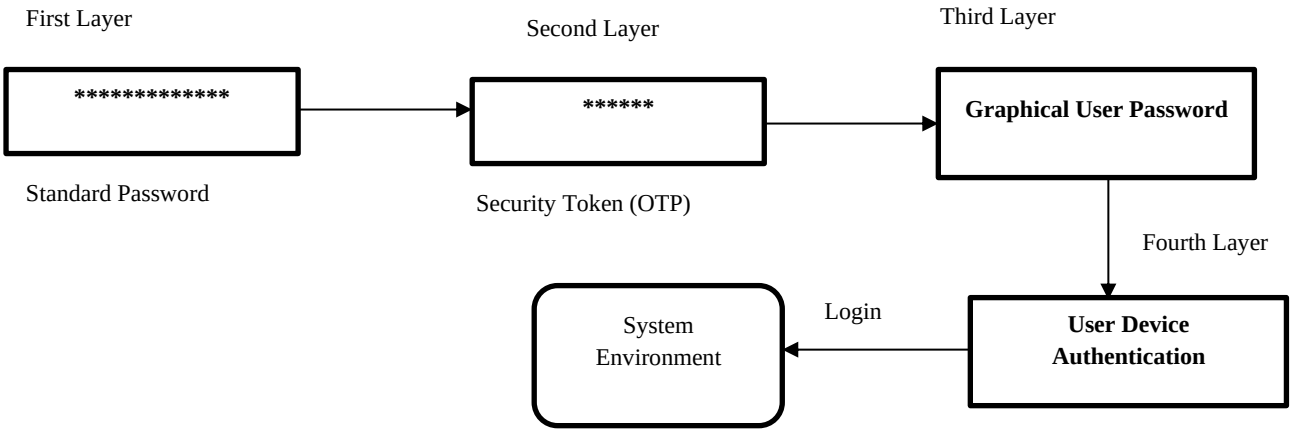

Figure 1: The block diagram of the proposed scheme

2.1 Formal Security Analysis

This section provides the formal security analysis of the proposed security scheme using the BAN-Logic. It first describes the basic notation of BAN-Logic that was used to analyze the proposed scheme's secure authentication and correctness. These include:

i. Entities: Entities are represented using symbols like "N," "Q," "A," etc. These symbols represent participants or components in the system.

ii. Belief Operator (| ≡): The belief operator indicates that an entity believes in a certain statement or proposition. For example, N| ≡ statement means that entity N believes in the statement.

iii. Freshness (#): The freshness symbol "#" is used to indicate that a statement or message is fresh or newly generated.

iv. Banning Operator (⊲ban): The banning operator represents that an entity is banned for a certain duration. For example, N⊲ban(duration) signifies that entity N is banned for a specific time period.

v. Global Banning Operator (⊲global_ban): This operator indicates that an entity is globally banned for an extended duration due to exceeding ban thresholds.

vi. Recovery Operator (⊲recover): This operator represents the recovery mechanism for entities to regain access after being banned.

vii. Numerical Values: Numerical values like "max_attempts," "threshold," "global_ban_threshold," and "duration" are used to set limits, counts, and time periods in the logic.

viii. Authentication Phases: Terms like "username/password," "OTP," "graphical password," and "device authentication" represent different phases of the authentication process.

ix. Logical Operators: Logical operators such as ">, <", and "==" are used to express conditions and comparisons in the rules.

x. Duration Symbols: Symbols like "short_duration," "slightly_longer_duration," and "extended_duration" represent specific time periods for bans.

Thus, the rules below represent the BAN logic of the authentication system.

Rule 1: Username/Password Phase

If entity N fails the username/password phase authentication more than the allowed attempts, N's belief is updated to being banned for a short duration.

i. If N| ≡ #attempts(username/password) > max_attempts:

ii. N| ≡ N⊲ban(short_duration)

Rule 2: One-Time Password (OTP) Phase

If entity N fails the OTP phase authentication more than the allowed attempts, N's belief is updated to being banned for a short duration.

i. If N| ≡ #attempts(OTP) > max_attempts:

ii. N| ≡ N⊲ban(short_duration)

Rule 3: Graphical User Password Phase

If entity N fails the graphical user password phase authentication more than the allowed attempts, N's belief is updated to being banned for a short duration.

i. If N| ≡ #attempts(graphical password) > max_attempts:

ii. N| ≡ N⊲ban(short_duration)

Rule 4: Device Authentication Phase

If entity N fails the device authentication phase more than the allowed attempts, N's belief is updated to being banned for a slightly longer duration.

i. If N| ≡ #attempts(device authentication) > max_attempts:

ii. N| ≡ N⊲ban(slightly_longer_duration)

Rule 5: Cumulative Global Ban

If entity N accumulates bans from all phases more than the global ban threshold within a certain period, N's belief is updated to being globally banned for an extended duration.

i. If #(ban phases) > global_ban_threshold within global_ban_period:

ii. N| ≡ N⊲global_ban(extended_duration)

Rule 6: Recovery Mechanism

Provide a mechanism for users to recover from bans.

i. N| ≡ N⊲recover

The BAN logic provides a comprehensive framework for reasoning about the security and correctness of the improved

3FA authentication system. The rules addressed different authentication phases, ban durations, cumulative global bans, and recovery mechanisms.

3.2 Informal Security Analysis

The proposed security scheme offers a robust defense against a range of security threats, including unauthorized access, Man-in-the-Middle attacks, privileged insider attacks, offline password guessing attacks, and stolen mobile device attacks. By combining multiple security layers and best practices, it enhances the security and integrity of the system, providing users with a reliable and secure experience.

Table 1 below shows the comparison of some security features of this scheme to other relevant schemes.

Table 1: Comparison of the proposed scheme with other relevant schemes based on security features.

Security Features	Saqib et al. [12]	Moon et al. [10]	Fakroon et al. [11]	Proposed Scheme
Man in the middle attack	Yes	Yes	Yes	Yes
Resistance to user impersonation attack	Yes	No	No	Yes
Secure login and password change phase	Yes	No	Yes	Yes
Privileged insider and offline password guessing attack	Yes	No	No	Yes
Resistance to stolen mobile device attack	No	No	No	Yes
User Experience	No	No	No	Yes

3.2.1 Man-in-the-middle attacks

If an attacker attempts to capture and modify a message M1 = {C9, C10, C11} as it traverses our security layers:

C9 represents the standard username and password layer, which acts as the first line of defense. Even if the attacker captures this, they cannot easily decipher the password or username due to strong encryption. C10 corresponds to the one-time password (OTP) layer. It is time-sensitive and unique for each session, making it challenging for the attacker to predict or reuse. So, C10 = R1, where R1 is the randomly generated OTP for that session. C11 involves cryptographic hashing with the secret key Ss and the random value R1. The attacker cannot compute C10 = R1, nor can they deduce C11 = h [(Ss) ‖ R1], because they lack knowledge of Ss and R1. This ensures that even if they capture C11, they cannot reverse engineer the OTP or compromise the message integrity.

Similarly, the attacker cannot modify other messages:

M2 = {Z, C12}: C12 represents the graphical password layer. The attacker cannot easily decipher or replicate the graphical password without specific user interaction. Therefore, our proposed scheme resists modifications to C12.

M3 = {C13, X, C14}: C13 and C14 involve additional layers of encryption or authentication that the attacker cannot bypass without the necessary credentials or devices.

M4 = {W, B}: These elements also include device authentication and secure communication. Unauthorized devices (B) cannot gain access, and secure communication (W) prevents tampering or eavesdropping.

M5 = {Y, C15, C16}: C15 and C16 are protected by the same security layers as previously described, making it challenging for the attacker to manipulate these messages.

Thus, our implemented authentication scheme resists Man-in-the-Middle attacks by incorporating multiple security layers, including strong encryption, time-sensitive OTPs, graphical passwords, and device authentication. These layers collectively deter attackers from capturing, modifying, or deciphering messages at various stages of communication, ensuring the integrity and security of the system.

3.2.2 Resistance to User Impersonation Attack

The scheme resists user impersonation attacks by combining multiple layers of security. Each layer (C1, C2, C3, and C4) adds a unique barrier that the attacker must overcome to successfully impersonate a user. This multi-factor approach makes it significantly difficult for attackers to gain unauthorized access and impersonate legitimate users, ensuring the security and integrity of the system.

3.2.3 Secure Login and Password Change Phase

The security layers in our proposed scheme ensure secure login and password change phases is as shown below:

i. Secure Login Phase

a. Standard Username and Password (C1):

During the login phase, the user enters their standard username and password (C1). The system verifies the credentials against a securely stored database. This process ensures that only authorized users can access the system.

b. Resistance to unauthorized access:

The system authenticates the user based on their valid username and password (C1).

c. One-Time Password (OTP) (C2):
In addition to the standard credentials, users also enter a time-sensitive OTP (C2) generated for that specific login session.

The OTP provides an extra layer of security, making it challenging for attackers with stolen credentials to gain access.

d. Resistance to stolen credentials:

An attacker with stolen credentials (C1) cannot log in without the valid, time-sensitive OTP (C2).

e. Graphical Password (C3):

Some users may use a graphical password (C3) as an additional layer during login. This graphical password adds a unique and personalized layer of security.

f. Resistance to unauthorized access:

The system verifies the user's graphical password (C3) to further ensure the user's identity.

ii. Secure Password Change Phase

a. Password Change Process (C1):

To change the password, the user must log in using their existing credentials (C1). The system authenticates the user's identity before allowing them to proceed with a password change.

b. Resistance to unauthorized password changes:

Only the legitimate user with their current credentials (C1) can initiate a password change.

c. One-Time Password (OTP) for Password Change (C2):

During the password change phase, users may receive a separate OTP (C2) for added security. This OTP ensures that even if an attacker somehow gains access to the user's login credentials (C1), they cannot change the password without the OTP.

d. Resistance to unauthorized password changes:

The system requires the valid OTP (C2) to confirm the password change.

Thus, our scheme ensured a secure login phase by combining standard credentials (C1) with time-sensitive OTPs (C2) and optional graphical passwords (C3). This multi- factor authentication process enhances the security of user logins. Additionally, during the password change phase, users must pass through similar security layers. This ensures that only legitimate users can change their passwords, and even then, they must have access to the OTP (C2) for added security. The combination of these security layers in both login and password change phases helps protect user accounts from unauthorized access and maintains the integrity of the system.

3.2.4 Privileged Insider and Offline Password Guessing Attack

The security layers in our proposed scheme defend against privileged insider attacks and offline password guessing attacks is described below:

a. Defense Against Privileged Insider Attacks

Standard Username and Password (C1): Privileged insiders are individuals who have authorized access to the system. Even if they know the standard username and password (C1) of another user, they still need to bypass additional security layers.

i. Resistance to insider attacks: Knowing someone else's username and password (C1) alone doesn't grant privileged insiders access to other user accounts.

ii. One-Time Password (OTP) (C2): During login, even privileged insiders must provide a valid OTP (C2) generated for that specific session. OTPs are time-sensitive, so even if an insider has access to a user's C1, they cannot use it to impersonate the user without the current OTP (C2).

iii. Resistance to unauthorized access: Privileged insiders need both the valid C1 and the current, time-sensitive OTP (C2) to gain access.

iv. Graphical Password (C3): If users employ graphical passwords (C3), it adds an extra layer of security. Privileged insiders would still need to replicate the specific graphical password, which is unique to each user.

v. Resistance to unauthorized access: Even privileged insiders must have the user's unique graphical password (C3) to gain access.

b. Defense Against Offline Password Guessing Attacks

i. Strong Password Policies (C1): Users are encouraged to create strong, complex passwords as part of C1. Strong passwords are resistant to offline guessing attacks because they are difficult to crack.

ii. Resistance to password guessing: Offline attackers face a formidable challenge in cracking strong, complex passwords.

iii. One-Time Password (OTP) (C2): OTPs (C2) are generated for each session and are not reused.

Even if an attacker captures an OTP, it's useless for future logins, making offline guessing attacks futile.

iv. Resistance to offline attacks: OTPs (C2) are effective against offline attackers since they cannot be reused.

Our scheme was designed to resist both privileged insider attacks and offline password guessing attacks. It employs multi-factor authentication with OTPs (C2), strong password policies (C1), and optional graphical passwords (C3) to ensure that even individuals with insider access cannot easily gain unauthorized entry. Additionally, strong password policies and the use of OTPs make offline password guessing attacks impractical, as the credentials and OTPs are time-sensitive and difficult to crack. This multi-layered approach helps maintain the security and integrity of the system.

3.2.5 Resistance to Stolen Mobile Device Attack

The security layers in our proposed scheme resist attacks when a mobile device is stolen:

i. Device Authentication (C4): Each mobile device is authenticated with the system through device-specific credentials and identifiers (C4). If a mobile device is stolen, the thief lacks the necessary device-specific credentials and identifiers to gain unauthorized access.

ii. Resistance to unauthorized access: Stolen mobile devices cannot be used to access the system without the legitimate device's unique authentication (C4).

iii. One-Time Password (OTP) (C2): Mobile devices often receive OTPs (C2) via SMS or dedicated apps. In case of a stolen mobile device, the attacker may obtain previously sent OTPs. However, OTPs are time-sensitive and cannot be reused for future logins.

iv. Resistance to unauthorized access: Even with captured OTPs from the stolen device, the attacker cannot log in without

the current OTP (C2).

v. Remote Device Management and Locking: The system can implement remote device management features. If a mobile device is stolen, the legitimate user or system administrator can remotely lock or wipe the device, preventing unauthorized access.

vi. Resistance to unauthorized access: Stolen devices can be remotely secured to protect sensitive data and prevent access to the system.

Our implemented authentication scheme is designed to resist stolen mobile device attacks effectively. Device authentication (C4) ensures that even if a device is stolen, it cannot be used to access the system without the legitimate device-specific credentials. OTPs (C2) add an extra layer of security, as they are time-sensitive and cannot be reused, even if captured. Additionally, the system can employ remote device management and locking features to further enhance security in the event of a stolen device. This multi-layered approach helps safeguard user accounts and system integrity when mobile devices are compromised.

4. IMPLIMENTATION AND RESULTS

The scheme was implemented using software development tools. They include: PHP, Flutter and Java Script Programming tools, My Structured Query Language (MySql) and PhPAdmin database applications, and Visual code editor development tool. The screenshots of the implementation are as shown in figures 2 to 5.

The figures above represent the registration pages for the intended user of the IoT device. Each graphic image is divided into four segments (figure 2) and the user is expected to choose any one of it. The process is repeated for the other three images one of which is shown in figure 3.

Figure 4 shows the first layer of the user login page, where the user of the IoT device is expected to supply their username and password before proceeding to the next layer. Once the user fails to supply the correct credentials an automated message is sent to the user's email recommending for change of password if they are not the one trying to login to the system. Figure 5 shows the second layer of the user login page, where a One-Time-Password (OTP) is sent to the user registered email address, which the user is required to input in the text field as shown in Figure 1 above. Once the user fails to supply the correct OTP, the process is halted and an automated message is sent to the user's email recommending for change of password if they are not the one trying to login to the system. Figure 6 shows the graphical authentication layer of the user login page, where the user of the IoT device is expected to select from the displayed graphical images the exact images and portions of the

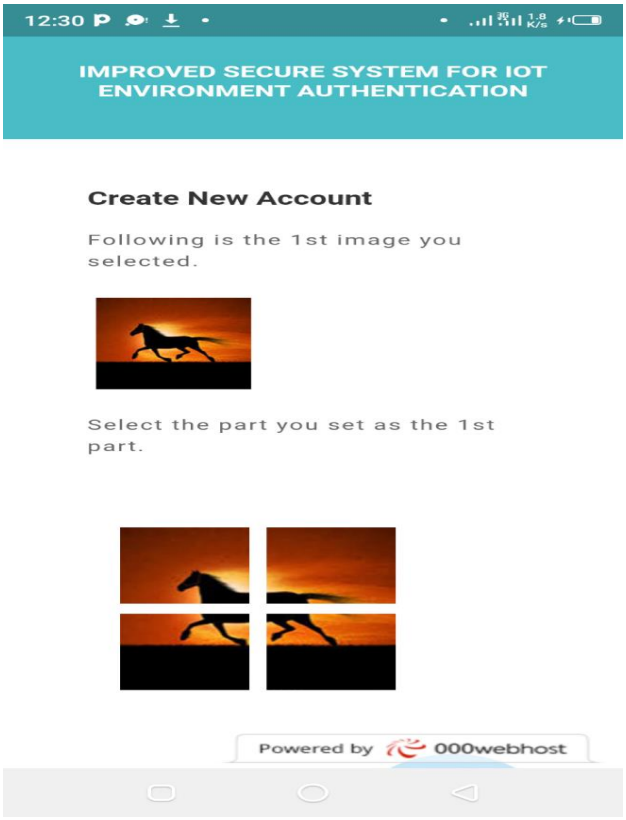

Figure 2: First graphical password

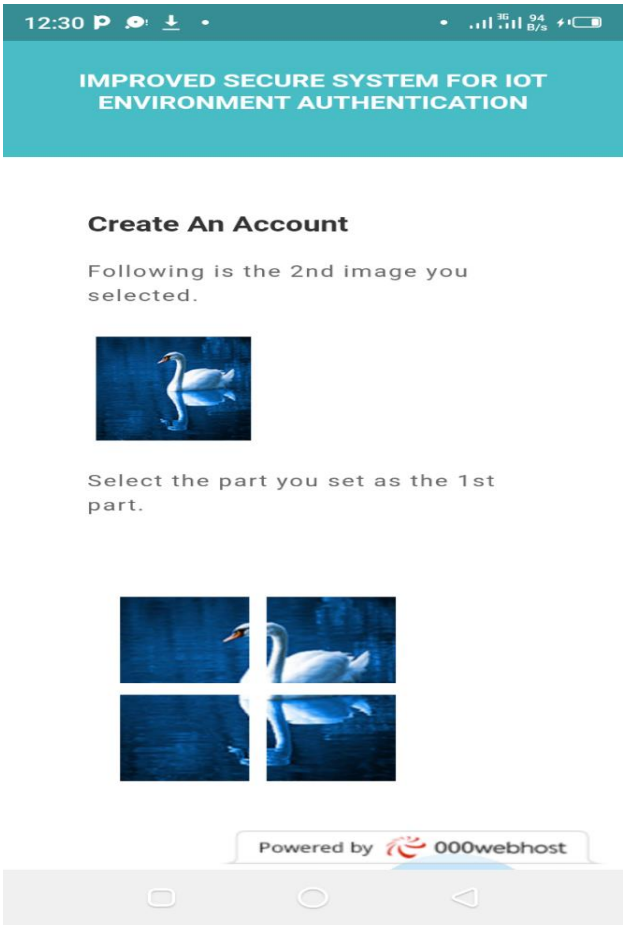

Figure 3: Second graphical password

segmented images as selected during the registration process proceeding to the next layer. Once the user fails to supply the correct credentials, access to the resource(s) is denied, otherwise the user is allowed to continue with the transaction.

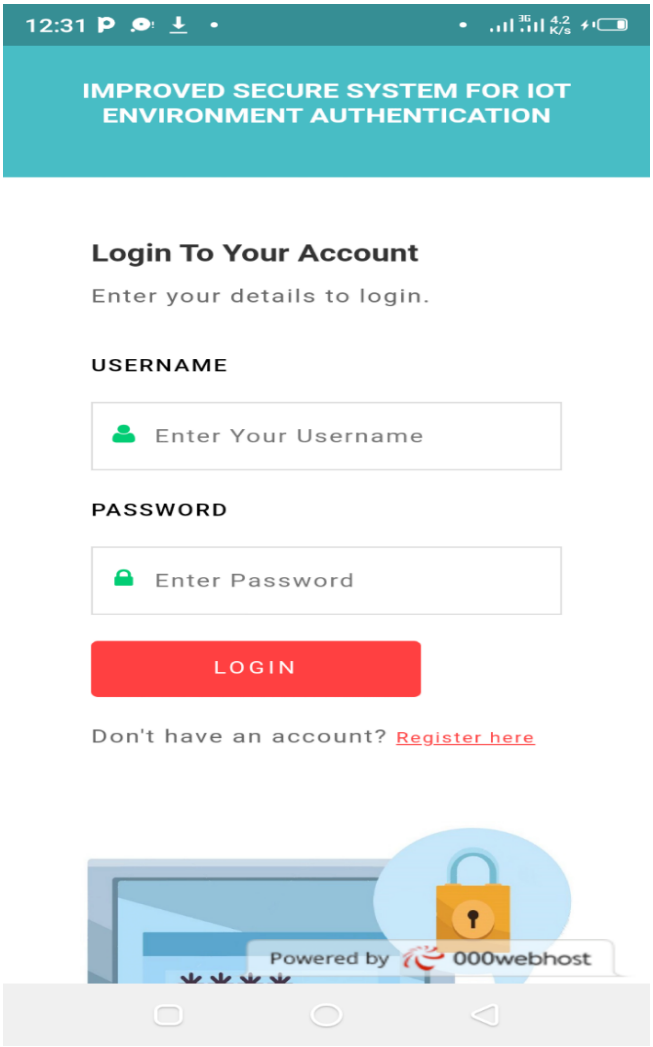

Figure 4: First Layer Login Page

5. CONCLUSION AND FUTURE WORKS

This study focused on fortifying IoT authentication security by addressing the vulnerabilities posed by Man-in-the-middle (MitM) attacks. Its objectives were accomplished through a multifaceted strategy that commenced with an exhaustive review of existing three-factor authentication (3FA) systems within IoT, establishing fundamental design requirements and principles. Subsequently, a novel 3FA algorithm was conceived, aligning closely with these identified prerequisites and implemented using the PHP programming language. Rigorous performance evaluations were conducted, underscoring the algorithm's robust capabilities. By delineating crucial design requirements, this study laid a solid foundation for crafting a resilient solution. The development and successful implementation of a tailored 3FA algorithm, meticulously designed to meet these requirements, served as a practical testament to its feasibility and functionality. While the improved 3FA algorithm showcased promising outcomes, its validation in real-world IoT environments remains pivotal. Future research avenues should explore large-scale

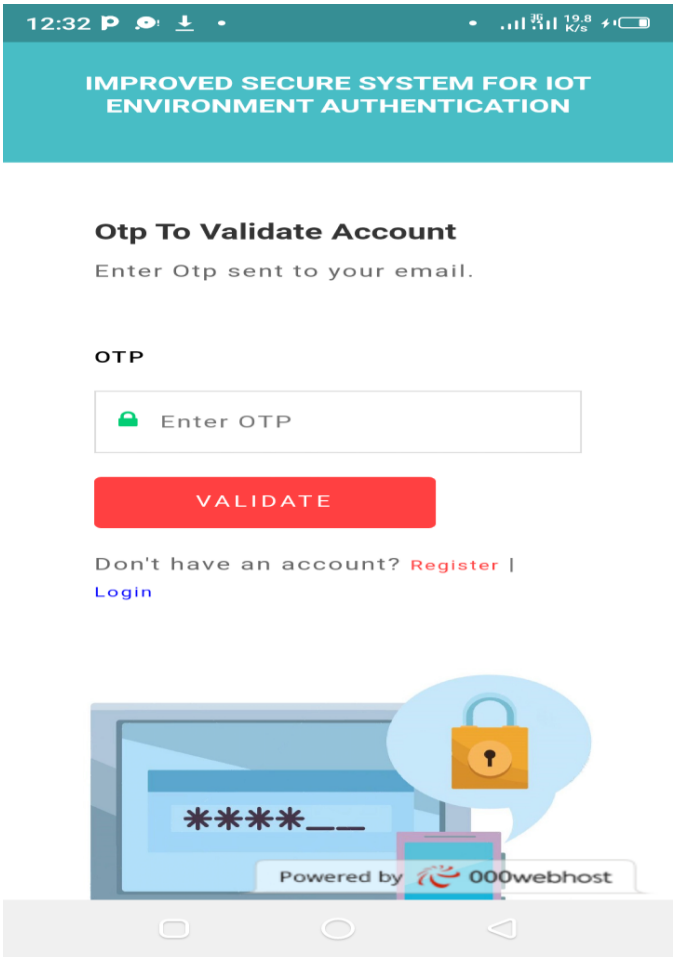

Figure 5: Second Layer Login Page

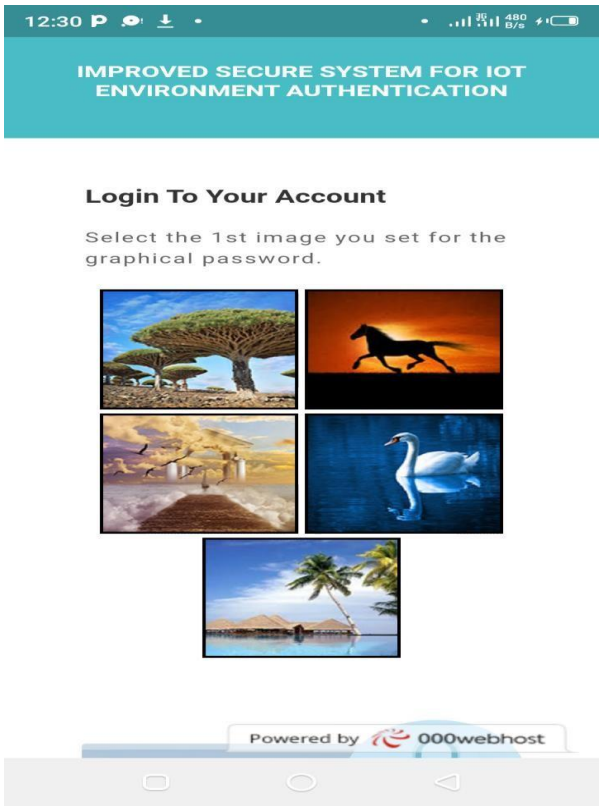

Figure 6: Graphical User selection

deployments, rigorously testing the algorithm's performance across diverse network conditions and varied device setups. This comprehensive evaluation will ascertain its effectiveness in practical IoT scenarios, further solidifying its role in bolstering IoT authentication security. Furthermore, a more extensive evaluation considering various datasets or scenarios would enhance this study in the future.

6. REFERENCES

[1] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking," IEEE Internet Things J., vol. 5, no. 6, pp. 4829–4842, 2018, doi: 10.1109/JIOT.2018.2846040.

[2] A. Giri, S. Dutta, S. Neogy, K. Dahal, and Z. Pervez, "Internet of things (IoT): A survey on architecture, enabling technologies, applications and challenges," ACM Int. Conf. Proceeding Ser., 2017, doi: 10.1145/3109761.3109768.

[3] M. G. Samaila, M. Neto, D. A. B. Fernandes, M. M. Freire, and P. R. M. Inácio, "Challenges of securing Internet of Things devices: A survey," Secur. Priv., vol. 1, no. 2, pp. 1–32, 2018, doi: 10.1002/spy2.20.

[4] B. H. Taher, H. Liu, F. Abedi, H. Lu, A. A. Yassin, and A. J. Mohammed, "A Secure and Lightweight Three-Factor Remote User Authentication Protocol for Future IoT Applications," J. Sensors, vol. 2021, 2021, doi: 10.1155/2021/8871204.

[5] Z. Sharmin, R. M. Noor, T. K. Soon, I. Ahmedy, N. A. Abdullah, and Y. S. Poh, "IoT Based Multidimensional Mushroom Waste Management System in Urban Area," 2021 3rd Int. Conf. Sustain. Technol. Ind. 4.0, STI 2021, vol. 0, pp. 18–19, 2021, doi: 10.1109/STI53101.2021.9732609.

[6] A. Ullah, M. A. Hossain, N. Zaman, M. Dey, and T. Kundu, "Enhanced Women Safety and Well-Suited Public Bus Management System in Bangladesh Using IoT," Adv. Internet Things, vol. 09, no. 04, pp. 72–84, 2019, doi: 10.4236/ait.2019.94006.

[7] Shamshad, S., Mahmood, K., & Kumari, S. Comments on "A Multi-factor User Authentication and Key Agreement Protocol Based on Bilinear Pairing for the Internet of Things." In Wireless Personal Communications (Vol. 112, Issue 1). 2020. https://doi.org/10.1007/s11277-020-07038-2

[8] Y. Zhang, J. Xu, Z. Wang, R. Geng, K.R. Choo, J. Perez-Diaz & D. Zhu, "Efficient and Intelligent Attack Detection in Software Defined IoT Networks," 2020 IEEE Int. Conf. Embed. Softw. Syst. ICESS 2020, 2020, doi: 10.1109/ICESS49830.2020.9301591.

[9] M. Rana, A. Shafiq, L. Altaf, M. Alazab, K. Mahmood, S.A. Chaudry, Y.B. Zikria, "A secure and lightweight authentication scheme for next generation IoT infrastructure," Comput. Commun., vol. 165, no. November 2020, pp. 85–96, 2021, doi: 10.1016/j.comcom.2020.11.002.

[10] J. Moon, D. Lee, Y. Lee, & D. Won, "Improving biometric-based authentication schemes with smart card revocation/reissue for wireless sensor networks". Sensors (Switzerland), 17(5). 2017, https://doi.org/10.3390/s17050940

[11] M. Fakroon, M. Alshahrani, F. Gebali, & I. Traore, "Secure remote anonymous user authentication scheme for smart home environment", Internet of Things (Netherlands), 9. 2020, https://doi.org/10.1016/j.iot.2020.100158

[12] M. Saqib, B. Jasra, & A. H. Moon. "A lightweight three factor authentication framework for IoT based critical applications", Journal of King Saud University - Computer and Information Sciences, 34(9), 6925–6937, 2022, https://doi.org/10.1016/j.jksuci.2021.07.023