EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

# Privacy Preserving Authentication of IoMT in Cloud Computing

G. Misra[1,*], B. Hazela[2] and B.K. Chaurasia[3]

[1]Department of Computer Science and Engineering, Amity School of Engineering & Technology Lucknow, Amity University, Uttar Pradesh, India
[2]Department of Computer Science and Engineering, Amity School of Engineering & Technology Lucknow, Amity University, Uttar Pradesh, India
[3]Department of Computer Science and Engineering, Pranveer Singh Institute of Technology, Kanpur, U.P., India
[1]garima.misra@s.amity.edu, [2]bhazela@lko.amity.edu, [3]brijeshchaurasia@ieee.org

## Abstract

INTRODUCTION: The Internet of Medical Things (IoMT) blends the healthcare industry with the IoT ecosystem and enables the creation, collection, transmission, and analysis of medical data through IoT networking. IoT networks consist of various healthcare IT systems, healthcare sensors, and healthcare management software.
OBJECTIVES: The IoMT breathes new life into the healthcare system by building a network that is intelligent, accessible, integrated, and effective. Privacy-preserving authentication in IoMT is difficult due to the distributed communication environment of heterogeneous IoMT devices. Although there has been numerous research on potential IoMT device authentication methods, there is still more to be done in terms of user authentication to deliver long-term IoMT solutions. However, password handling is one of the big challenges of IoMT.
METHODS: In this paper, we present an IoMT-related online password-less authentication technique that is quick, effective, and safe. In order to offer cross-platform functionality, the article includes a simulation of FIDO2/WebAuthn, one of the most recent standards for a password-less authentication mechanism.
RESULTS: This makes it easier to secure user credentials and improve them while preserving anonymity. The IoMT device authentication process and registration process delays are also assessed.
CONCLUSION: Results and simulations show that the efficacy of the proposed mechanism with quick authentication on cloud servers may be accomplished with the fewest registration and authentication procedures, regardless of device setup.

**Keywords:** FIDO2 (Fast IDentity Online), WebAuthn (Web Authentication), IoMT (Internet of Medical Things), ECDAA (ECC based DAA algorithm)

Received on 25 February 2023, accepted on 12 October 2023, published on 03 06 2024



doi: 10.4108/eetiot.6235

*Corresponding author. Email: garima.misra@s.amity.edu.

## 1. Introduction

IoMT has completely transformed the health care environment by using Internet-connected medical equipment to remotely connect patients with healthcare providers [1]. IoMT devices gather medical information from patients and provide it to healthcare professionals for analysis in order to detect diseases at an earlier stage. In respect to IoMT, patient data security is of utmost concern: with the first level of security necessary to safeguard being entity authentication [2]. The entity may be the user, an IoMT device, smart watch, etc. Secure IoMT authentication is difficult due to the variety of devices and limited resource availability. The most widely used technique of device authentication at present is password authentication, an approach which has several flaws. Due to the widespread use of passwords on digital platforms, phishing attempts sometimes involve impersonating websites [3]. In order to ensure user security and privacy, it is necessary to lessen the reliance on password-based authentication for access to online services [4]. By moving verification to the device rather than exchanging

credentials through the internet, the password-less authentication approach alters the underlying security architecture.

The COVID-19 pandemic has once again emphasized the significance of intelligent healthcare services which provide remote prevention, diagnosis, and treatment [5]. The concept of "smart healthcare" encompasses more than just technological advancements in the healthcare industry. Users frequently use the same passwords across numerous websites, making them vulnerable to man-in-the-middle assaults and easy for attackers to crack.

Password entry through human interaction and multiple password memories become time-consuming and expensive tasks [6]. The security of users' data is weakened by storing passwords in a database. Users are looking for ubiquitous authentication to make their daily lives easier while maintaining the highest level of security and network privacy.

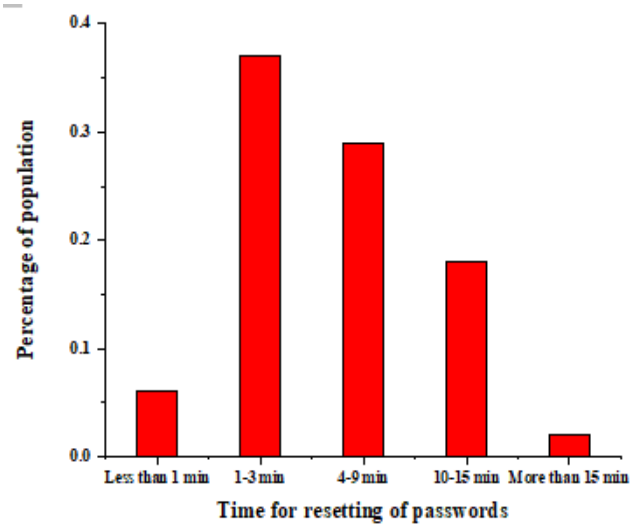


**Fig.1** Cracking Time of Passwords [8].

Fig. 1 shows the cracking time of a password based on its strength. The average weekly time spent entering and resetting passwords is slightly over 12 minutes. In comparison to two years earlier, 63% of respondents stated they were more concerned about the security and privacy of their personal data [8].

Devices centered around passwords are susceptible to phishing attacks, where intruders deceive users into revealing their credentials and compromising security. Malware, keyloggers, or other malicious software can steal passwords from user devices, compromising the entire IoMT ecosystem [7]. Attackers can exploit human vulnerabilities to trick users into disclosing their passwords or other sensitive information. Some IoT and medical devices may have limited input options, making it difficult to implement strong password policies effectively. In the event of a password breach, it can take time to detect unauthorized access, allowing attackers to cause damage or access sensitive data before being detected.

In this paper, we suggest a password-less, privacy-preserving authentication method that uses a single passkey to verify multiple devices in an IoMT environment. In order to facilitate cross-platform interoperability, we employ the FIDO2 protocol, which is based on public-key cryptography. Registered and authenticated devices with the FIDO2/WebAuthn protocol set up and using passkeys [8].

The authenticator scans QR codes to create passkeys, which are subsequently used to establish signatures. The FIDO2 protocol is an online authentication system that allows users to confirm their identities to servers using a hardware credential called an authenticator. Additionally, we looked at how long it took to register and authenticate using FIDO2/Web Authn, employing passkeys which do away with password-based authentication and need human interaction at the very first login across several platforms. Section 2 of this paper includes related work, problem formulation is discussed in Section 3 and in Section 4, we introduced the proposed methodology of work, including detailed information about FIDO2/WebAuthn protocol and the ECDAA scheme. In Section 5 and 6, result evaluation is followed by the conclusion

## 2. Related Work

The preexisting literature has suggested a number of IoT authentication schemes; however, there aren't many password-less solutions to be found there. There are various methods used for IoT device authentication and authorization, however.

Decoy strategy in combination with fog computing facility is one methodology for securing patients' MBD in the healthcare cloud [9]. It functions as a second gallery to house dummy MBDs (DMBDs), which give the attacker the impression that the real MBDs (OMBDs) are located there. Rachakonda, L. *et al* [10] offer a workable method for sharing medical records in the cloud while protecting privacy. By vertically partitioning the medical dataset based on the categorization of the qualities of medical records, it has achieved consideration of various components of medical data with various privacy issues. Amendola, S. *et al* [11] suggest a system verification protocol that authenticates the network's devices without keeping data in memory. PUFs are used to give each device in the network a distinct identity and to provide authentication while sending data to the server. Hossain, S. *et al* [12] introduced a device authentication protocol for an IoMT device network that can strengthen system security and make the network impervious to such attacks. Regardless of the protocol used for communication between the end device and the server, this protocol can be used. No information about the end device is immediately saved on the server, which further protects the surrounding system.

Through inexpensive, energy-free, and disposable sensors, RFID technology is now developed enough to supply a portion of the IoT physical layer for personal

healthcare in smart surroundings. State-of-the-art RFID technology for usage in body-centric systems and for obtaining data (temperature, humidity, and other gases) about the user's living environment has been surveyed [13]. The proposal of an ECC based secure verification, permission, and key management scheme for wireless sensor networks in 5G-integrated IoMT [14] provides a secure and efficient scheme analysis. One-time certificates can be created for just one line verification, applying the Zero Knowledge technique in order to correctly recover the unique identifier and the Hardware Media Access Control key which are used in Yubico [15] for the client's gadget calculation. Given that OTKs can be used again as necessary and kept on consumer gadgets, the current research highlights reliable data retrieval though falls short in appropriately addressing safety issues.

A different endeavor proposes to use Application as a Service and Two Factor Authentication to eliminate the complexity of credential verification in a server-based system [16]. For imitation incidents, the system demonstrates its strength [17]. This biometric certificate-driven approach blocks several online services. Online-based data storage is susceptible to intrusions and assaults.

This matter of safety has additionally been investigated [18], suggesting the use of an outline for multi-factor authentication and multiple login controls to verify users' identities. Techniques for encryption and methods for encoding are employed to help prevent data or information leaks. In order to identify malicious users, suggested approaches and strategies have demonstrated significant detection rates and misleading alert rates [19].

Current PUF-based gadget verified credential transfer systems with multiple layers of authentication were presented in another study with the ability to mutually verify a server safely [20]. For a multiple-factor verifier driven FIDO application system the client's gadget serves as an authenticator. The system is employed to set up encrypted connections between IoT gadgets and the platforms [21]. Microsoft has been actively promoting FIDO2 as part of its password-less authentication strategy. In healthcare, Microsoft's Azure AD supports FIDO2 for secure access to healthcare applications and services. Organizations using Microsoft's healthcare solutions can leverage FIDO2 for enhanced authentication [35].

Some other authentication approaches are also available for IoMT, such as the zero-knowledge-based scheme [36] and the infrastructure-aided scheme [37]. All these schemes suffer from password handling issues. As a result, a password-less authentication scheme, especially for IoMT, is needed. In this work, we have proposed a password-less approach which can address the above issue.

## 3. Problem Formulation

IoMT devices can connect to the cloud using any desktop or laptop with an open shared wireless environment. When working with private medical data in the IoMT context, there may be a number of security issues, including the following:

In the first place, if malevolent cyberattacks can commandeer medical sensors affixed to a person's body, this may not only lead to erroneous information gathering but also jeopardize the patient's condition. Second, malevolent hacks may reveal private medical and patient data. Third, while IoMT relies on minimal-power medical sensors worn on body parts, the protocol utilized may be too heavy to function regularly or to offer real-time service because it requires laborious calculation. In order to prevent data breaches and man-in-the-middle attacks and to provide secure cross-platform device authentication, there is a need for effective, straightforward password-less authentication for IoMT devices.

## 4. Proposed Methodology

The use of cloud computing and FIDO2 to authenticate IoMT devices while maintaining their privacy is covered in this section [22]. FIDO2 makes phishing-resistant authentication features on Internet of Medical Things devices more widely accessible. Using an instance of the JavaScript API that websites can utilize to link to such authenticators and perform cryptography with a public key authorization, Fig. 2 demonstrates how authentication devices may interact with clients.

The suggested technique uses cloud-based technology for multi-platform, secure IoMT verification using multi-device certificates (passkeys). IoMT devices present at the edge layer are able to authenticate without a username and password with the use of passkeys. The cross-platform interoperability problem is resolved by passkeys, which also support multi-device credential services.

The procedure consists of four parts: (a) Trusted Third Party, (b) WebAuthn framework, (c) Android phone, (d) a quick response code. In order to build Passkeys for authenticators (IoMT devices like smart watches, smart sugar glucometers, and Android phones), we considered the platform (Windows 11) with the WebAuthn API and search engine backed by FIDO that display QR codes. As wandering authentication systems for the smart watch (a wearable IoMT device), Android phones have been considered.

A camera-based authenticator analyses a short code to produce login credentials for authenticating the gadget. They keep a set of values known as a public-private key pair that is specific to a person, a web page, or security issuer. The client provides the web page with the public key during the sign-up process. The client then delivers the tool, a proof of ownership each time he desires to sign in, verified with his confidential key, which the application can then validate using the user's public key from when he logged in, demonstrating that the user is the true proprietor of the related private key. A user's device or system can connect with an authenticator via the Client-to-Authenticator Protocol Version 1 (CTAP1) [23]. It permits

either internal or external authenticators, such as those found in laptops or handheld devices, for computer applications and web services that employ the Web Authentication (WebAuth) protocol established by the W3C. IoMT devices can communicate with other devices over Bluetooth (BLE) since they are not required to register a credential on every page they visit.

When authenticating on a web-based platform or trusted third party where the authentication device has been authenticated, a WebAuthn login is utilized. The intelligent gadget then decides to sign in using attributes from next generation, such as a key that is publicly accessible [24]. The internet page requests for the usage of a set of keys that tests the verifier.

Whether orally or through an electronic motion the consumer grants permission for the utilization of the private key. The authentication system checks the website's URL.

If the provided URL is linked to an encrypted key pair, the authenticator only responds to the objection and generates an acknowledgment that has been verified with the secret key. The website verifies the digital fingerprint using a publicly accessible key assigned to the client and issuer upon authorization.

The individual is permitted to sign in if both the query's reply and the signature are legitimate. For authenticator certification, the previously described ECDAA algorithm [25] is utilized. This proposed solution makes use of a collaborative passkey via a QR Code to accomplish privacy. In the part that follows, the recommended solution's detailed process is provided.

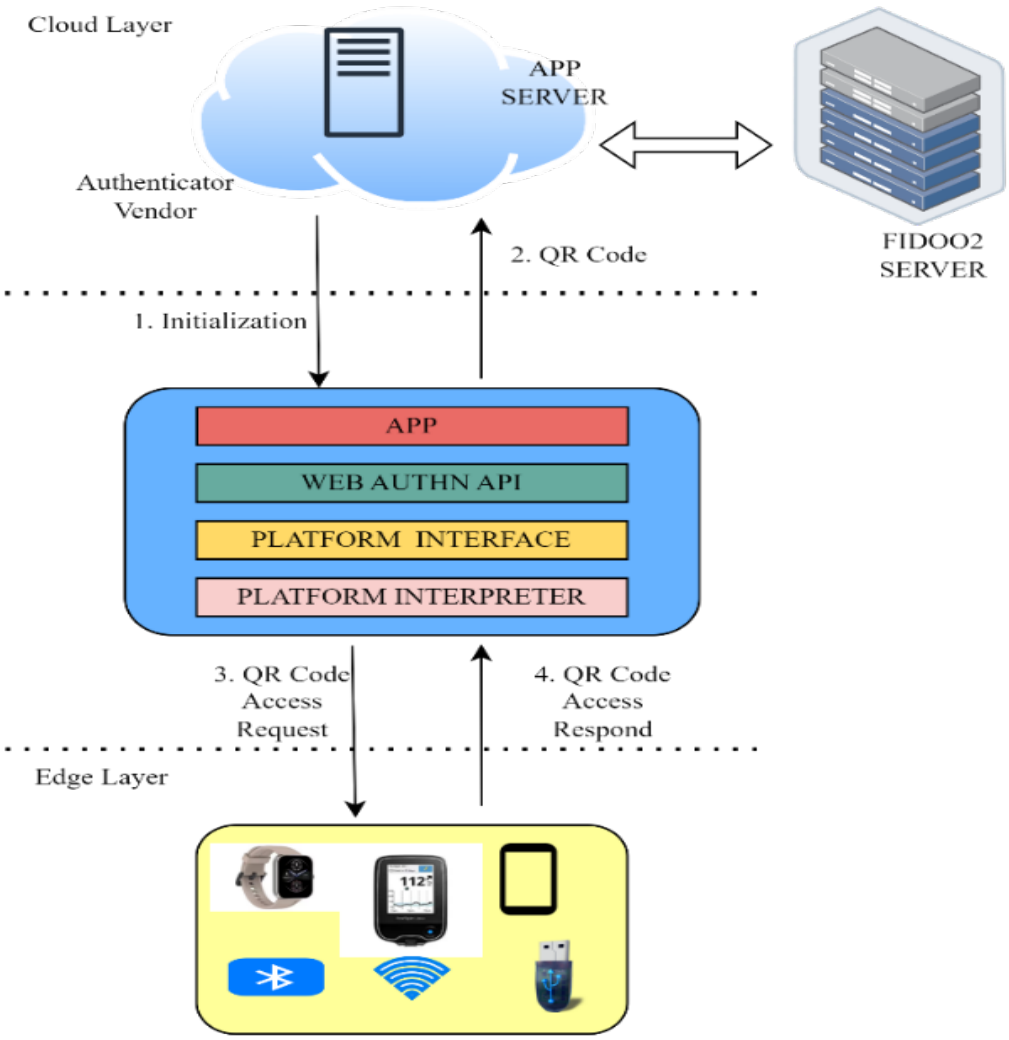


**Fig. 2.** The privacy-preserving authentication of IoT using cloud computing.

## 4.1 Working Process of Proposed Methodology

We have developed the FIDO2-QRCode authentication protocol, which employs passkeys to provide multi-device credentials generated by a trusted platform module (TPM) and consequently improves device security, as a result of our examination of the most recent FIDO specification, FIDO2/WebAuthn.

The proposed privacy-preserving authentication of IoT using cloud computing mechanism shown in Fig. 3 contains the following steps:

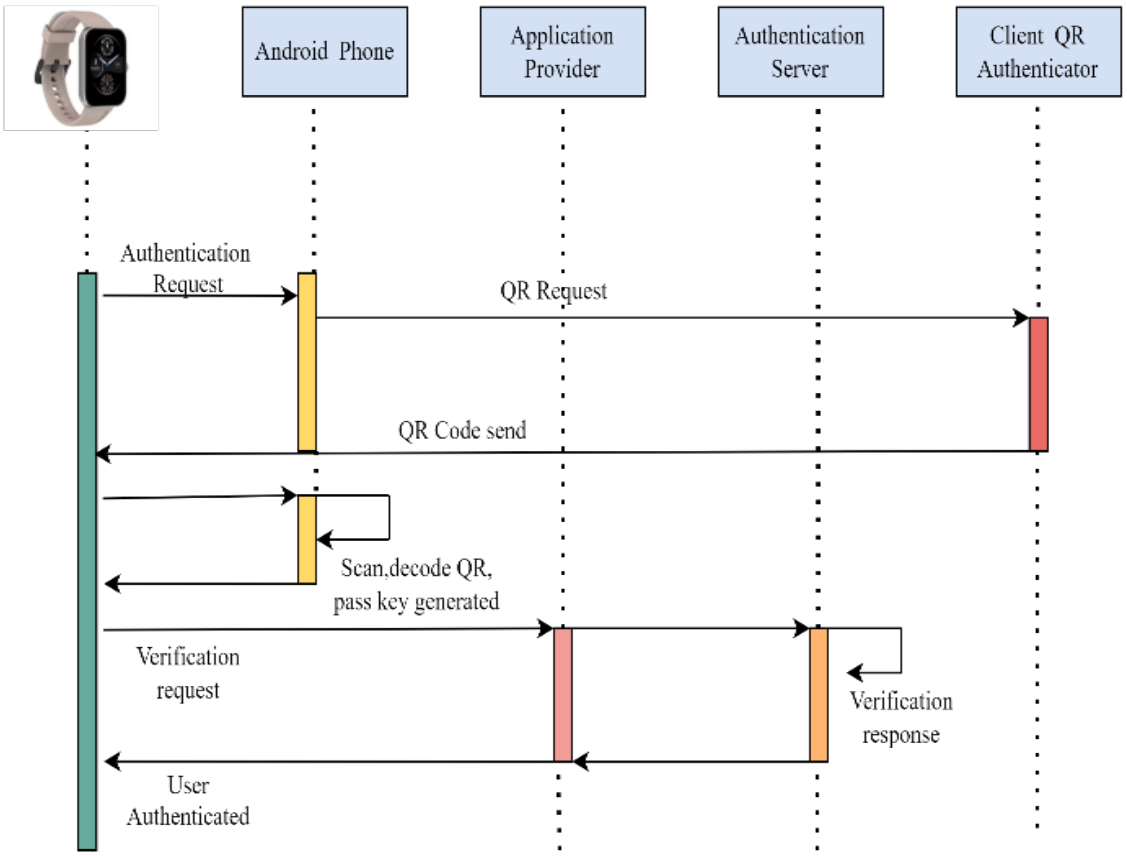


**Fig.3** Privacy-Preserving Password-less Authentication

1. $D_i$ starts the registration process for a client $QR$ authenticator $QR_a$ present in the cloud. A user starts the authentication process by connecting their account to the application provider (web API on the gateway as any laptop or server), which is also known as a trusted third party ($TTP$).
2. In response to a request from user $D_i$, $QR_a$ creates a random token in the form of a $QR$ code ($QR_{code}$). It will only become accessible after one of the protection certificates for the smartphone or tablet, a personal identification number pattern matching, or the person's face lock, has been entered. The program developer might offer a FIDO login criterion describing the qualities needed to authenticate the gadget.
3. In response to a request from user $D_i$, $QR_a$ creates a random token in the form of a $QR$ code ($QR_{code}$). It will only become accessible after one of the protection certificates for the smartphone or tablet, a personal identification number pattern matching, or the person's face lock, has been entered. The program developer might offer a FIDO login criterion describing the qualities needed to authenticate the gadget.
4. After the Gateway application provider has verified the security credentials of $D_i$ (a IoMT device), $TTP$ sends $D_i$ a $QR_{code}$. A nonce, or the accepted certificate, which has a time of termination, is also included in the $QR_{code}$. In order to provide multi-device credentials, the $QR_{code}$ is kept in the smartphone as Passkeys. We

presume that the trusted platform ($TP$) on the smartphone and gateway is activated. After three stages, the registration procedure is finished.

5. Instead of being kept on a cloud server, Passkeys are kept on the client's gadget as a secret key after matriculation.
6. The sign-in process is then started by $D_i$, who also sends a verification request to $TTP$, who then forwards it to the authentication server. The reply is validated by the authentication server.
7. After the verification response has been provided to the $TTP$, a message confirming authentication is subsequently sent to the users' mobile devices.

## 4.2 FIDO- Direct Anonymous Attestation Scheme

We have developed the FIDO2-QRCode authentication protocol, which employs passkeys. Using credentials provided by the group management (the issuer), the direct anonymous attestation scheme ($DAA$) is a unique group technique that may be used to verify that a signature was issued by an authorised group member [26]. The group manager, however, cannot tell who signed a signature if it is authentic, in contrast to earlier group signing methods [27].

In order to provide the relying party with cryptographic proof of the authenticator model, FIDO and FIDO2 make use of the concept of attestation. When the authenticator is registered with the reliant party ($TTP$), the certification statement, also called as a key registration data object (KRD), contains the public key of a new authentication key pair. When utilising the ECDAA Algorithm (Elliptic Curve Direct Anonymous Attestation) [28] with ECDAA-Sign, the KRD object is signed. The elliptic curve (E) is the foundation of the DAA scheme [29], and pairings are referred to as ECC-DAA. Compared to other traditional attestation techniques, ECC-DAA is more cost-effective in terms of compute, storage, and communication.

Global system parameters and $ECDAA$ Issuer-specific parameters are defined by $ECDAA$ certification. On the server, the verifier, and the FIDO System, both parameter sets must be installed. There are two steps in the $ECDAA$ method:

Before the initial FIDO Registration, an ECDAA-Join must be completed between the authenticator and the $ECDAA$ Issuer. When supplying the credentials to vouch for the authenticator model, the $ECDAA$ Issuer acts in the vendor's place.

$$(n, B, s_c, y_c) = Get\ Nonce\ from\ ECDAA\ Issuer()$$

$$(D = Q, c1, s1) = ECDAA\ Join(X, Y, B, s_c, y_c, n)$$
$$(A, B, C, D) = ECDAA\ IssuerJoin(Q, c1, s1)$$

$$ECDAA\ Join2(A, C)\ //store = (A, B, C, D)$$

And, the set of $ECDAA - Sign$ carried out by the verifier and $ECDAA - Verify$ carried out by the dependent party's FIDO System as an element of FIDO Identification.

$$Client\ Attestation = (signature, KRD)$$
$$= ECDAA\ Sign(AppID)$$

$$Server: SuccessECDAAVerify(signature, KRD, AppID)$$

*Global ECDAA System Parameters:*

1. Three groups of prime order $x$ are selected as $A_1, A_2\ and\ A_T$.
2. The generators $G_1\ and\ G_2$ are defined satisfying the following condition: $A_1 = G_1\ and\ A_2 = G_2$.
3. A bilinear pairing $b: A_1 * A_2 \rightarrow A_T$.
4. A hash function such that $h: \{0,1\}^* \rightarrow Z_x$.
5. A hash function $h_{A_1}: \{0,1\}^* \rightarrow A_1$.
6. $(A_1, G_1, x, h, h_{A_1})$ are installed in the authenticators.

*ECDAA Join*

The authenticator must first obtain $ECDAA$ credentials from an $ECDAA\ Issuer$ in order to use $ECDAA$. The $ECDAA - Join$ operation does this. Before the first credential registration may happen, this process must be done just once.

After the $ECDAA - Join$, the authentication device will use the $ECDAA - Sign$ procedure as a component of every FIDO Registration. This process does not involve $ECDAA\ Issuer$. In FIDO Authentication and Transaction Confirmation procedures, ECDAA has no bearing. $ECDAA$ requires the use of at least one $ECDAA\ Issuer$ [30]. The strategy outlined in this document is easily scaled to include numerous $ECDAA\ Issuer$, such as one for each authenticator provider. FIDO permits the authenticator vendor to select any $ECDAA\ Issuer$, equivalent to his current ability to choose any PKI architecture or company to provide the validation credentials required for FIDO Standard Authentication. One of the $ECDAA\ Issuer$ entities is used for all $ECDAA - Join$ actions (of the linked authenticators).

Public parameters, or $ECDAA$ public key material, are available to each $ECDAA\ Issuer$ Each authenticator model, identified by its AAGUID, contains the corresponding Attestation Trust Anchor in its metadata.

1. The B value of the certificate is requested by the verifier from the $ECDAA\ Issuer$ .
2. The $ECDAA\ Issuer$ selects a integer value $n$ such that $n = RAND(x)$.
3. The value of B is calculated by the following statement $B = h_{A_1}(n)$
4. The value of $s_c and\ y_c$ are send to the authenticator.
5. The value of private key is selected as $s_k = RAND(x)$ and is stored.

6. The authenticator recomputes the value of

$$B = h(s_c, y_c)$$

7. The value of public key is computed as

$$Y = B^{s_k}.$$

8. The knowledge of $s_k$ is verified by the following terms:

$$Biginteger\ i_1 = RAND(x)$$
$$ECpoint\ V_1 = B^{i_1}$$
$$Biginteger\ c_2 = h(V_1|X_1|Y|n)$$
$$Biginteger\ m = RAND(x)$$
$$Biginteger\ c_1 = h(m|c_2)$$
$$Biginteger\ s_1 = i_1 + c_1.s_k$$

9. The authenticator then sends the value of $(Y, c_1, s, m)$ to the ASM which forward it to the $ECDAA\ Issuer$
10. The authenticator is confirmed to be "authentic" and that $Y$ was truly created by the authenticator by the $ECDAA\ Issuer$. This might be simple for an in-factory join, but for a distant join, it usually necessitates the employment of additional cryptographic techniques. Unlikability is not an issue for $ECDAA - Join$ since it is a one-time operation.
11. $ECDAA - Sign$ : For the client-side environment, just one $ECDAA - Sign$ procedure is necessary each time a new password is saved at a trusted party.
12. $ECDAA - Verify$ : Each FIDO Registration must include one $ECDAA - Verify$ operation for the FIDO Server. Both the Ecc-Daa credential and the signature itself are checked as part of this process [31]. Keep in mind that the Verifier requires access to keys X and Y that belong to the Issuer. Along with the data required for confirming the various signatures. If two signatures corresponding J and K values are identical and not different, the Verifier can also determine whether the two signatures are linked.

## 5. Result Analysis

In this section, the results of the proposed privacy-preserving authentication of IoMT in cloud computing is analyzed.

*Performance Evaluation*

We examined the duration of processing for four distinct IoMT products' enrolment and verification on an online service or TTP, which was implemented with a FIDO server, in order to assess the effectiveness of our suggested protocol. Every gadget is subjected to numerous tests, and the mean duration is calculated and examined. Passkeys make authenticating an equipment easier, quicker, and less user-interactive.

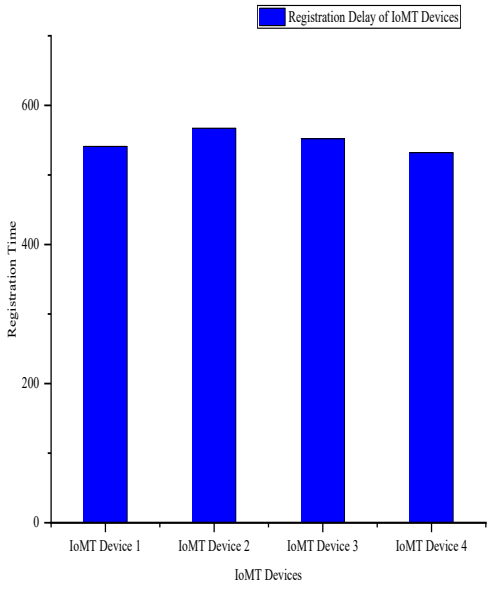


**Fig. 4.** Registration Process on Cloud Server

Fig. 4 depicts the registration delay calculated for the four IoMT devices which have different specifications. The IoMT devices are used as authenticators and time consumed in each devices varies according to the device and its specifications. The registration process is performed at the cloud server and it is observed that almost all the devices consume same registration time with just small variations. The maximum time taken for registration by an IoMT device is 576 milliseconds, this is the time taken for the first-time registration by the device using its passkey.

To avoid having to register every device to a user account numerous times, multi-device credentials are kept using passkeys. When compared to other ExtraF Models, Multi-platform authentication with scalability and compatibility is possible using Passkeys [32]. Cryptographic keys help counter replay attacks where attackers attempt to replay captured authentication data. The unique private key prevents such impersonation attempts. FIDO2's integration of cryptographic keys and biometric factors in smartwatch authentication offers a robust security framework. The combination of strong cryptographic principles and unique biological traits fortifies the authentication process, ensuring only authorized users and devices can access sensitive data and services on the smartwatch.

Fig. 5 shows the authentication delay of every IoMT device on the trusted third party which is obtained after the process of registration of all four IoMT devices. It is observed that the time taken for the authentication of each device is less than compared to its registration time. In the DAA scheme the public key is matched and only the authentic user is verified by the process. [33]. All the devices do not take more than 538 ms for the process of the authentication at the server. The authentication time

needed by the device is also affected by the unlocking feature or the specifications of the mobile devices and hence it varies from device to device. However, two factor authentication [13] is required to store passwords in any memory at any place that is suffering from stolen passwords, key management problems, and update problems. The proposed scheme is complete in order of milliseconds and able to overcome the existing issue of [13]. Mitigating phishing and credential-based attacks is crucial for ensuring the security of systems and protecting sensitive information. FIDO2, with its modern authentication approach, plays a significant role in addressing these security challenges. FIDO2 relies on public-key cryptography, where each user device generates a unique key pair. The private key remains on the device and is never shared, making it extremely difficult for attackers to duplicate it. FIDO2 employs a challenge-response mechanism during authentication. Even if a user unknowingly responds to a phishing attempt, the response is useless without the correct challenge, providing an additional layer of security.

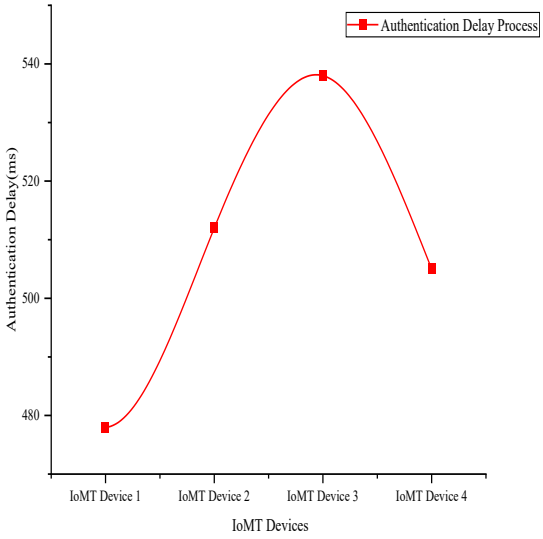


**Fig. 5.** Authentication Process on Relying Party

## 6. Conclusion

The development of a secure IoMT-based system to safeguard the confidentiality of crucial and sensitive patient data seems more sensible in light of the recent advent and widespread use of IoMT, particularly during the COVID-19 pandemic. It has been discovered that the great majority of IoMT security measures are susceptible to a number of attacks, including quantum assaults. To protect users' data and identities, the authentication mechanism must therefore be strengthened [34]. In this research, we investigated the FIDO2 protocol-based password-less authentication solution offering cross-platform functionality. The roaming authenticator (Android phone) generated $\mathcal{QRCode}$ to produce passkeys that support multi credential device features.

Multiple IoMT devices are registered and authenticated on the FIDO Server-based $TTP$ to estimate the performance of the FIDO2 registration and authentication processes. The ECC-DAA approach describing a security element to authenticate diverse IoMT devices in a cloud context is also covered in our work.

The Direct Anonymous Attestation approach, which also keeps the user-transmitted message and id to TTP, demonstrates the user's privacy. When compared to competing protocols, FIDO2/WebAuthn shines out due to its speedy registration and authentication procedures despite low user participation and ordinary computer specifications.

Future development will involve deploying a variety of additional devices as authenticators to create numerous keys for FIDO2 multi-platform authentication. Additionally, we anticipate utilizing an assessment system to demonstrate the FIDO2 protocol's accessibility, safety flaws, and finally develop a prototype to verify the efficacy of proposed scheme.

## References

[1]. J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano.: The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In IEEE Symposium on Security and Privacy, May 2012

[2]. F. M. Farke, L. Lorenz, T. Schnitzler, P. Markert, and M. D¨urmuth.: You still use the password after all–Exploring FIDO2 Security Keys in a Small Company. In Symposium on Usable Privacy and Security, August 2020.

[3]. K. S. Killourhy, and R. A. Maxion.: Comparing anomaly-detection algorithms for keystroke dynamics. In IEEE/IFIP International Conference on Dependable Systems and Networks, June 2009.

[4]. W. Oogami, H. Gomi, S. Yamaguchi, S. Yamanaka, and T. Higurashi.: Observation study on usability challenges for fingerprint authentication using WebAuthn-enabled android smartphones. In Symposium on Usable Privacy and Security, August 2020.

[5]. Yadav, V. K., Yadav, R. K., Chaurasia, B. K., Verma, S., Venkatesan, S.: MITM Attack on Modification of Diffie-Hellman Key Exchange Algorithm. In 2nd International Conference on Communication, Networks & Computing (CNC-2019), 144-155 (2022). https://doi.org/10.1007/978-981-16-8896-6_12.

[6]. H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren, and A. Alamri.: A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography. In IEEE Access, vol. 5, pp. 22313–22328, 2017.

[7]. J.-J. Yang, J.-Q. Li, and Y. Niu.: A hybrid solution for privacy preserving medical data sharing in the cloud environment. In Future Gener. Comput. Syst., vols. 43–44, pp. 74–86, Feb. 2015.

[8]. G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner.: Smart locks: Lessons for securing commodity

internet of things devices. In *Proceedings of the 11th ACM Asia Conference on Computer and Communications Security, ASIA CCS 2016*, pp. 461–472, Xi'an, China, June 2016.

[9]. V. P. Yanambaka, S. P. Mohanty, E. Kougianos and D. Puthal.: PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things. In *IEEE Transactions on Consumer Electronics*, vol. 65, no. 3, pp. 388-397, Aug 2019.

[10]. L. Rachakonda, P. Sundaravadivel, S. P. Mohanty, E. Kougianos and M. Ganapathiraju.: A Smart Sensor for Stress Level Detection in IoMT. In *Proceedings of the 4th IEEE International Symposium on Smart Electronic Systems (iSES)*, pp. 141-145, December 2018.

[11]. S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi and G. Marrocco.: RFID Technology for IoT-Based Personal Healthcare in Smart Spaces. In *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 144-152, April 2014.

[12]. Hossain, S., Goh, A., Sin, C. H., Win, L. K.: Generation of one-time keys for single line authentication. In14th Annual Conference on Privacy, Security and Trust (PST), 1-4 (2016) https://doi.org/10.1109/PST.2016.7906957

[13]. Chaurasia, B. K., Shahi, A., Verma, S.: Authentication in Cloud Computing Environment using Two Factor Authentication. In 3rd International conference on soft computing for problem solving (SocProS2013), 2, 779-786, (2014) https://doi.org/10.1007/978-81-322- 1768-8_67

[14]. Said, W., Mostafa, E., Hassan, M. M., 1 Mostafa, and A. M.: A Multi-Factor Authentication- Based Framework for Identity Management in Cloud Applications. In Computers, Materials & Continua Tech Science Press, 71 (2), 3193-3209, (2022) https://doi.org/10.32604/cmc.2022.023554

[15]. Yubico, Online available at: https://www.yubico.com/press-releases/yubicos-2019-state-of- password-and-authentication-security-behaviors. Accessed 19 May 2023.

[16]. Top two hundred most common password, Online available at: https://nordpass.com/most- common-passwords-list/Fasdf. Accessed 29 March 2023.

[17]. Murmu, S., Kasyap, H. & Tripathy, S. PassMon.: A Technique for Password Generation and Strength Estimation. J Netw Syst Manage 30, 13, (2022) https://doi.org/10.1007/s10922-021- 09620-w

[18]. Tripathi, S., Singh, V. K., Chaurasia, B. K.: An energy-efficient heterogeneous data gathering for sensor-based internet of things. In Multimedia Tools and Applications , 1-24, (2023) https://doi.org/10.1007/s11042-023-15161-y

[19]. Hossain, S., Goh, A., Sin, C. H., & Win, L. K.: Generation of one-time keys for single line authentication. In 2016 14th Annual Conference on Privacy, Security and Trust (PST) IEEE, 686-689 (2016) https://doi.org/10.1109/PST.2016.7906957

[20]. Said, W., Mostafa, E., Hassan, M. M., & Mostafa, A. M.: A multi-factor authentication-based framework for identity management in cloud applications. CMC-Computers Materials & Continua, 71(2), 3193-3209, (2022) http://dx.doi.org/10.32604/cmc.2022.023554

[21]. Musumeci, F., Fidanci, A. C., Paolucci, F., Cugini, F., & Tornatore, M.: Machine-learning- enabled DDoS attacks detection in P4 programmable networks. Journal of Network and Systems Management, 30, 1-27, (2022) https://doi.org/10.1007/s10922-021-09633-5

[22]. Shahidinejad, A., Ghobaei-Arani, M., Souri, A. Shojafar, M., Kumari, S.: Light-Edge: A Lightweight Authentication Protocol for IoT Devices in an Edge-Cloud Environment. In Ali IEEE Consumer Electronics Magazine, 1-6 (2021) https://doi.org/10.1109/MCE.2021.3053543

[23]. FIDO Alliance. Available online at: https: //fidoalliance.org/. Accessed 11 April 2023.

[24]. W3C, Available online at: https://www.w3.org/2019/01/webauthn-extensions.html. Accessed 21 April 2023

[25]. FIDO Alliance. Available online at: https://fidoalliance.org/specs/fido-v2.1-ps- 20210615/fido-client-to-authenticator-protocol-v2.1-ps-errata-20220621.pdf. Accessed 11 April 2023

[26]. Bachl, M. (2016). The end of the password era: towards password-less authentication based on enhanced FIDO (Doctoral dissertation, Wien).

[27]. FIDO Alliance. Available online at: https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-ecdaa-algorithm-v2.0-id-20180227.html

[28]. FIDO Alliance. Available online at: https://fidoalliance.org/passkeys/

[29]. Togan, M., Chifor, B. C., Florea, I., Gugulea, G.: A smart-phone based privacy-preserving security framework for IoT devices. In 9th IEEE International conference on electronics, computers and artificial intelligence (ECAI), 1-7 (2017). https://doi.org/10.1109/ECAI.2017.8166453

[30]. FIDO Alliance. Available online at: https: //fidoalliance.org/members/. Accessed 03 April 2023

[31]. FIDO Alliance. Available online at: https://fidoalliance.org/fido2/. Accessed 03 April 2023

[32]. FIDO Alliance. Available online at: https://fidoalliance.org/specifications/. Accessed 17 April 2023

[33]. W3. Available online at: https://www.w3.org/2019/03/pressrelease-webauthn-rec.html. Accessed 07 April 2023.

[34]. FIDO Alliance. Available online at: https: //fidoalliance.org/. Accessed 11 April 2023.

[35]. FIDO Alliance. Available online at:

[36]. https://fidoalliance.org/specs/fido-v2.0-id- 20180227/fido-client-to-authenticator-protocol-v2.0-id-20180227.html. Accessed 20 April 2023

[37]. Misra, G., Hazela, B., & Chaurasia, B.K.: Zero Knowledge based Authentication for Internet of Medical Things. In 14th International Conference on Computing, Communication and Networking Technologies (ICCCNT), IIT - Delhi, Delhi India, 1-6 (2023). DOI: 10.1109/ICCCNT56998.2023.10307359

[38]. Chaurasia, B.K. & Verma, S.: Infrastructure based Authentication in VANETs. In International Journal of Multimedia and Ubiquitous Engineering, 6(2), 41-54, 2011.