FIDO based Password Less Authentication System for E-Bikes

M. Gopinath [1], Uday Kiran Pillala [2*], Umesh Meduri [3]

[1,2,3] Department of Artificial Intelligence and Data Science, Siddhartha Academy of Higher Education, Vijayawada, Andhra Pradesh, India

* pillalauday2005@gmail.com

* Corresponding author
doi: https://doi.org/10.21467/proceedings.7.6.8

Abstract

Recently, E-Bikes (electric bikes) are widely used in the market. The method of user authentication is crucial for electrical bikes. Once the user has successfully completed the authentication process to confirm their login, they can use the bike. Despite the availability of numerous authentication systems, ID/PW authentication remains popular due to its low cost and convenience. However, users who employ ID/PW techniques are not very secure. The passwords can be cracked by the illegitimate people and they can use the electric bikes. As a result, we provide a FIDO-based password-less authentication system for securing electric bikes. It ensures strong and secure hardware-based authentication and resists various attacks related to traditional password authentication systems. The proposed mechanism ensured greater security for utilizing electric bikes effectively by using an application that enabled a hardware security key for login, which stored the passkey and was used at the time of login without requiring any password. In addition, the proposed authentication protocol is validated using AVISPA tool by feeding input in the format of HLPSL and obtained result as SAFE which implies that the proposed authentication protocol is highly secure against the vulnerable attacks like phishing, MITM and replay attacks.

Keywords: Electric bikes, Fast Identity Online (FIDO), Password-less authentication

1 Introduction

With the development of Technology today, E-Bikes are released into the market. In olden days the bikes run with the petrol and present there are bikes available that run with the electricity. Initially those bikes follow the old tradition of unlocking (starting the bike) by using key. Recently some bikes came into market those are unlocked by entering the password on the display of the bike and there is an option for unlocking through phone. Entering the password is crucial for unlocking those E-Bikes [1-3]. Despite the availability of numerous authentication methods, ID/PW authentication is the most popular due to its low cost. But employing the ID/PW authentication is not very secure. FIDO (Fast Identity Online) technology is an open standard for password less authentication. It modifies the traditional password-based authentication with methods such as biometrics (fingerprint, facial recognition) or hardware tokens (USB keys) [2]. There is a chance of cracking the password by other people illegally. The user has to remember the password to access the bike. Therefore, to reduce the risk of cracking the password and misusage of bike by others and user don't want to remember the lengthy passwords anymore.

In this paper, we proposed Fido based password less authentication system for E-bikes. Password less authentication involves security keys, biometric etc.… For Password less authentication there are some hardware security keys like YUBICO. First, we will set up the Fido Server for the Yubico - Security Key. There is an option of accessing E- Bike Through Mobile Phone So, by connecting this Yubico- Security Key to the mobile user can access the E-Bike without using Password. Hence the proposed mechanism will improve more security than traditional methods.

1.1 Motivation:

User authentication is one of the major factors affecting recent e-bikes. Although there are numerous methods there exist many flaws and difficulties in the authentication process. This approach will enhance the security over traditional methods like ID/PW authentication which was not secure due to development of technology. With today's technology it is very easy to crack the password. Hence, we proposed password less authentication to get more security for the bike.

Proceedings DOI: 10.21467/proceedings.7.6; Series: AIJR Proceedings; ISSN: 2582-3922; ISBN: 978-81-989164-9-5

1.2 Problem statement:

This study holds the Fido based password less authentication for E-Bikes. Fido technology is used for password less authentication for electric bikes.

1.3 Objectives:

- To enhance the security of the e-bikes.
- To replace the traditional authentication methods.
- To improve the authentication process for users.
- To Bypass the password-based authentication.
- Improved trends of password-less authentication

1.4 Contributions:

- Designed password-less authentication system for e-bikes using FIDO technology
- This authentication ensures more security than existing authentications.
- FIDO technology enhances security for authentication that uses two-factor authentication (2FA) and FIDO2 protocols.

2. LITERATURE SURVEY

Currently, the most used authentication method is the ID/password approach. To use this approach, the user needs a complicated combination of alphabetic letters, numbers, and special characters. Moreover, the user must frequently update their password to avoid the password guessing attack. However, remembering the complex password is challenging. To strengthen security, FIDO-based password management is used to overcome the inconvenience the users face in remembering passwords and password thefts [4]. A set of robust authentication protocol standards was suggested by Fido Alliance. There are two protocols, FIDO UAF Protocol and FIDO U2F (Universal Second Factor) Protocol, comprised in the FIDO architecture that address the two fundamental ways in which users might interact with internet services. Online services that offer multi- factor and password-free security are permitted by UAF. By incorporating an additional strong factor into the user log-in process, U2F targets online services to enhance the security of their current password architecture [5].

In the modern world, we have been using end-user authentication and other techniques in place of passwords, however, none of these techniques has been shown to be secure. Asymmetric cryptography-based protected connections are replacing password-based authentication as the main trend in the quickly evolving field of technology. The user authentication layer known as FIDO2 Kings has received greater attention in recent research. As said in knowledge-based authentication, the most widely used technique is one of several sophisticated distributed systems with growing user counts that flourish in the face of security issues and cyber threats. There are several benefits to utilizing this authentication mechanism, including its affordability, ease of usage, and user-friendliness [6]. Numerous flaws exist in the federated identity management (FIM) systems of today. Because the identity provider (IdP) is positioned at the hub of the identity ecosystem, their architecture is problematic. IdPs follow each user's login, invading their privacy. Like the most recent Facebook hack, they are also honeypots. Demonstrated, by giving the attacker access to the login for each service provider (SP) that the user had accounts with. Furthermore, malicious SPs can phish users' login credentials and usernames by redirecting them to the IdP. IdPs usually provide bearer identification assertions or tokens that have a brief lifespan and can be easily obtained and utilized by an adversary [7].

In addition to computers, everyone has cell phones and tablets these days. a number of web services that are accessible from these devices and that many educational institutions have introduced, including email, e-learning, and registration. Many organizations, including our university, have implemented integrated authentication infrastructures for the purpose of unifying authentication among web services. This allows for a streamlined login process while also enhancing authentication security. single sign-on (SSO) is made possible by integrated authentication infrastructure. With SSO, users just need to authenticate once to access numerous services. Moreover, there are issues with the password itself. Assume there are several services on an integrated authentication infrastructure that can be logged in via SSO. An identity and password pair that is compromised could be used fraudulently to log into any service. The LR-AKE technique was introduced as a two-factor authentication approach as a countermeasure. Nevertheless, the two-factor authentication approach hasn't yet completely resolved password issues [8]. After registering for a certain service, obtaining the security key is also cognitively simple. The term "brainless" used by Lang et al. to describe the use of security keys appears to imply the idea that security key adoption has no end points. But the Google paper was the only one we could find that listed adoption advantages [9].

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

A little hardware device called a YubiKey is used to verify a user's identity to network-based services. The YubiKey protocols have received very little security examination in the academic literature, despite being widely adopted (more than 20,000 clients, including Google and Microsoft, have received over a million devices sent by Yubico). Robert Kunnemann et al [10] identified the weaknesses in the established authentication protocols and suggested a secure authentication technique that leverages the Fido embedded Yubico key for enhanced security throughout the user authentication process. Table 1 provides the summary of related works.

Table 1. Summary of research works

S.No.	Research works	Key Focus	Authentication Method	Security Model	Cryptographic Techniques	Vulnerabilities Identified	Practical Applications
1	Kim et al. (2020)	FIDO, Smart Energy	FIDO UAF	MFA	Public Key	key storage and implementation flaws	Smart Energy Systems, IoT Security
2	Chadwick, D.W., et al. (2019)	Identity Management, Verifiable Credentials	FIDO UAF & U2F	Decentralized Identity Model	PKI	credential verification & interoperability issues	Digital Identity Management, Online Services Authentication
3	Das, S., et al. (2018)	Usability Study, Yubico Security Key	FIDO U2F (Hardware Token)	Usability & Human Factors	Challenge-Response	Usability concerns, loss of hardware token	Secure Web Authentication, MFA for Enterprises
4	Fink et.al. (2017)	Electric Vehicles, Usage Patterns	N/A	N/A	N/A	No major security concerns	Electric Mobility, Smart Grids
5	M. Morii et al. (2017)	Passwordless Authentication	Authentication	Integrated Authentication Framework	Public Key	Public Key Cryptography	Enterprise Security, SSO
6	Hu, K., Zhang, Z.	Security Analysis, FIDO UAF	FIDO UAF	Security Analysis	ECC	Possible replay attacks, key registration	Online Banking, Secure Web Transactions
7	Künneman n, R., Steel, G. (2021)	Security Analysis, Yubikey, YubiHSM	Hardware Security Module (HSM)	Formal Security Verification	AES, RSA, ECC	Key extraction, token cloning	Hardware Security, Cryptographic Key Management

2.1 Research Gap:

First and foremost, security is required to ensure user authentication and relieve users of the hassle of constantly changing their passwords. Combining these techniques should provide users of electric bikes with increased security and password less authentication. Second, while the mechanisms now in use for authentication do prioritize security, they are not very robust given the state of technology today. By eliminating the need for traditional passwords, password-less authentication is an emerging technology that promises to enhance security and user experience. Rather, it uses alternate techniques to authenticate users, such as hardware tokens, biometrics, one-time codes. An overview of the current technologies utilized in password-less authentication are Hardware tokens, email-based authentication, mobile-based authentication, and biometric authentication. The existing authentication techniques are ID/PW authentication for the E-Bikes. The traditional method is not very secure for authentication. Because, there is a chance of cracking the passwords by others. Hence, there is a need for new technology to enhance the security during authentication. We proposed a new method for authentication - A FIDO based password less authentication for E-Bikes. In this we use a security key that bypasses the password. Thus, it is necessary to explore the utilization of the current model for the purpose of authentication. Table 2 provides the performance comparison of FIDO with different features.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

Table 2: Comparison of performance with various features

Method\Feature	Password	Security	External key	2-Step Verification	Ease of Use	Authentication Factors	Phishing Resistance
Traditional	Required	Less Secure	Not required	User choice	Memorization required	Single-factor (password)	Vulnerable
FIDO based	Not required	More Secure	Required	Bulit in	Seamless	Multi-factor (biometric, security key, device)	Strong resistance

2.2 Tools Used:

The FIDO integrated Yubico-Security Key is used in this investigation. It is equipped with FIDO U2F/FIDO 2 Certified capabilities, a security key, USB-A or NFC connectivity, and two-factor authentication (2FA). required an application that supports the security key in order to use password less authentication.

3. Proposed FIDO based authentication System

3.1 Architecture

Fig.1&2. presents the registration and login phases of the proposed system respectively. This system is an enhancement to the Traditional ID/Pw system. which improves security for the E-bikes. Passwords serve as the primary authentication factor in electric bikes. To use the bike, users must be authorized through a user authentication procedure. Our solution makes use of the S-authenticator (Security authenticator), which securely saves the user's login details for alter-ego password. Our proposal consists of two schemes, i.e., s-auth registration, s-auth login. In ID/PW authentication, there are three components such as user, access device, service server. There are two additional components as shown in Fig 1&2. One is the S-authenticator to input the Security Key information. The other is S-auth client application to apply our methods with ID/PW authentication.

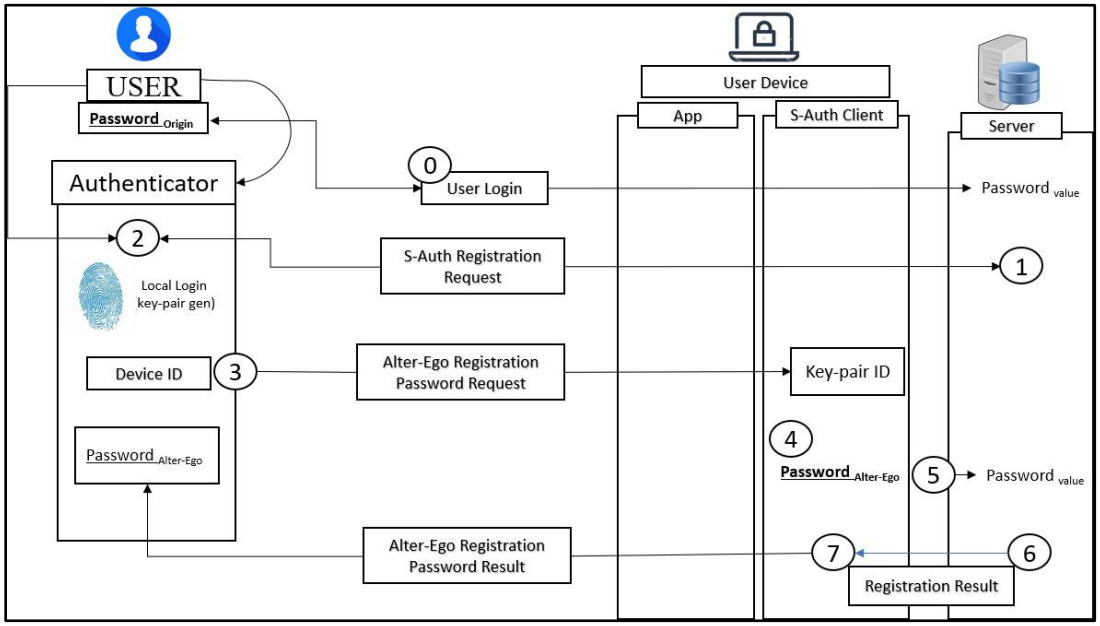

Fig. 1. Registration phase

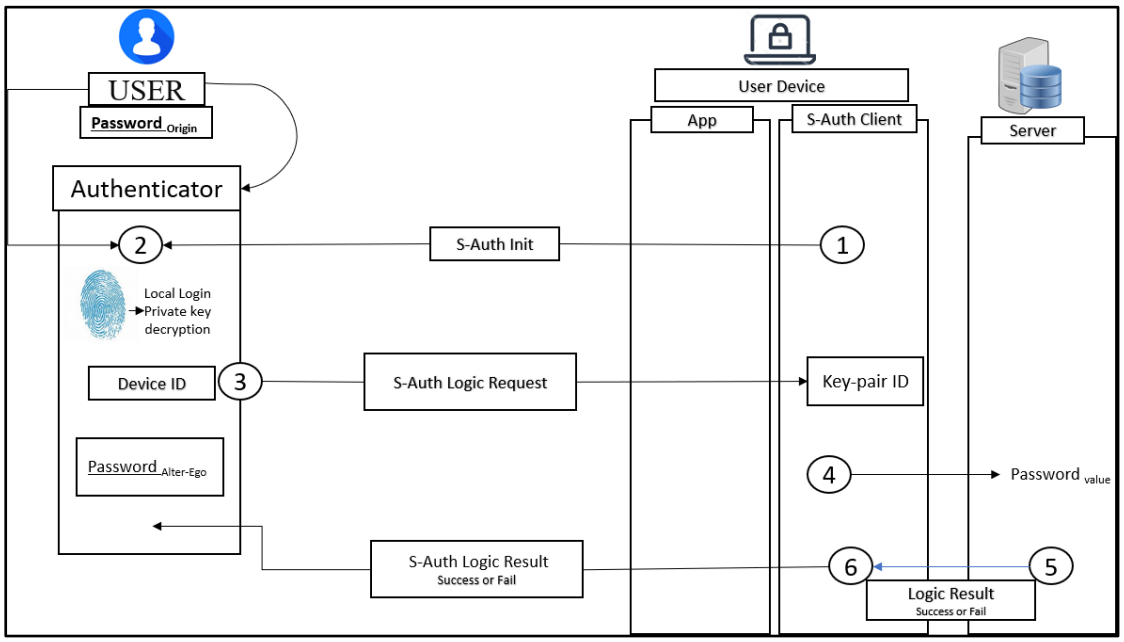

Fig. 2. Login and authentication phase

3.2 Methodology:

Implementing FIDO-based password less authentication involves integrating FIDO2/WebAuthn standards to enable secure, hardware-backed authentication for users. The process consists of several key steps, including system architecture design, implementation of authentication and registration flows, and security measures. Table 3 provides the notations of the proposed protocol and algorithm representations are given in table 4.

Table 3: Notation used in protocol

Notation	Description
U	User (Authorized E-Bike Owner)
EID	Relying Party ID of E-Bike system
EBS	Authentication Server of E-Bike
FA	FIDO Authenticator
PK	Public Key (Generated by FA)
SK	Private Key (Stored securely in FA)
N_1, N_2	Nonces (Random Challenges)
H(M)	Cryptographic hash function (SHA-256)
Sign_SK(M)	Digital signature using SK
Verify_PK(Sig, M)	Signature verification using PK
Cert_FA	Attestation Certificate (FIDO Authenticator)
$\oplus$	Concatenation operator

Design of Proposed system

To develop the propose system, the following elements needed for defining the authentication protocol.

- **User-Side:** An online or mobile interface where users start the registration or authentication process.
- **FIDO2 authenticator:** It can be a platform authenticator, a biometric-enabled device, or a hardware security key. The backend that handles user credentials, verifies authentication requests, and communicates with FIDO servers is known as the Relying Party (RP) server.
- **Identity Provider (IdP):** For federated login systems (like Google Passkeys), this is optional.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

The proposed authentication protocol is comprised with two phases which are registration phase and login and authentication phase and their functionalities are explained as following.

Registration Phase:

When a user enrols for the first time, they must register their FIDO2 authenticator. The steps to be followed are:

- ***User Initiates Registration:***
  - The user visits the registration page and enters their identifier (e.g., email, username) via mobile application or onboard interface of e-bike.

    U → EBS: Register_Request (U, EID)
- ***E-bike server Generates Challenge:***
  - The server generates a cryptographic challenge (a fresh 32-byte nonce) and sends it to the client via the WebAuthn API.

    EBS → U: $N_1 \leftarrow$ Random (32 bytes)

    EBS → U: Challenge_Request(N_1, EID)
- ***User Interacts with Authenticator:***
  - The user is prompted to use a FIDO2-supported authenticator (e.g., biometric authentication, USB security key, Bluetooth/NFC key). The authenticator generates a unique key pair (public/private) for the user and the e-bike system and signs the challenge.

    FA: (PK, SK) ← KeyGen(ECDSA_P-256)

    FA: Signed_N_1 = Sign_SK(H($N_1 \oplus$ EID))
- ***Signing and response:***
  - The authenticator sends the signed response and public key to the server. The server verifies the signature and associates the public key with the user's account.

    FA → U → EBS: {PK, Signed_N_1, Cert_FA}
- ***Registration Complete:***
  - The user is notified that registration is successful. The stored public key will be used for future authentication.

    EBS: Verify_PK(Signed_N_1, H($N_1 \oplus$ EID))

    EBS: If valid, store {U, PK, Cert_FA}

Table 4: Algorithm representation

Registration Phase (Key Pair Generation)		**Login and Authentication Phase (Challenge-Response Verification)**
Step 1: The user initiates registration on the e-bike's FIDO2-compliant system. **Step 2:** The e-bike's authentication server generates a **challenge** (random nonce) and sends it to the user's device (smartphone or onboard display) via WebAuthn. **Step 3:** The FIDO authenticator (e.g., security key or biometric sensor) generates a **public-private key pair** unique to the user and the e-bike system (Relying Party ID). **Step 4:** The authenticator **signs** the challenge using the private key and returns the signed response along with the public key to the e-bike's server. **Step 5:** The server verifies the signature and stores the **public key,** linking it to the user's e-bike profile for future authentication.		**Step 1:** The user attempts to log in e-bike by selecting "Sign in with FIDO" over their smartphone or onboard interface. **Step 2:** The e-bike's server generates a **cryptographic challenge** and sends it to the user's device via WebAuthn. **Step 3:** The FIDO authenticator **retrieves the stored private key** and signs the challenge. **Step 4:** The signed response is sent back to the e-bike's authentication server. **Step 5:** The server verifies the signature using the **previously stored public key**. If valid, authentication is successful, and access is granted by unlocking the e-bike for use.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

Login and Authentication Phase:

After registration, users can authenticate using their registered FIDO2 authenticator. The steps to be followed are:

- ***User Initiates Login (E-bike unlocking):***
  - The user selects the "Sign in with FIDO" option and enters their identifier on their mobile or onboard interface.

$$\mathbf{U \rightarrow EBS:}\ \text{Auth\_Request}(U, EID)$$

- ***E-bike's Server Generates Challenge:***
  - The relying party sends a cryptographic challenge to the client.

$$\mathbf{EBS \rightarrow U:}\ N_2 \leftarrow \text{Random(32 bytes)}$$

$$\mathbf{EBS \rightarrow U:}\ \text{Challenge\_Request}(N_2, EID)$$

- ***User Verifies Identity with FIDO Authenticator:***
  - The authenticator signs the challenge using the stored private key. The signed response is sent back to the server.

$$\mathbf{FA:}\ \text{Signed\_}N_2 = \text{Sign\_SK}(H(N_2 \oplus EID))$$

$$\mathbf{FA \rightarrow U \rightarrow EBS:}\ \{\text{Signed\_}N_2\}$$

- ***Server Validates Response:***
  - The server verifies the signature using the stored public key. If valid, authentication is successful, and the user is granted access for unlocking bike.

$$\mathbf{EBS:}\ \text{Verify\_PK}(\text{Signed\_}N_2, H(N_2 \oplus EID))$$

3.3 Multi-User Access

The proposed authentication mechanism allows multi-user access in which multiple users (U1, U2,..,Un) are securely authenticated and the e-bike can be unlocked by utilizing their unique FIDO authenticators. The are various advantages like shared e-bikes, lending e-bikes and multiple ownership environments.

4. Results And Analysis

The implementation of FIDO-based password less authentication for e-bikes enhances security by replacing traditional login methods with a hardware security key that securely stores passkeys. This approach effectively prevents, replay attacks, and unauthorized access by leveraging FIDO2 protocol. Unlike traditional methods such as PINs, RFID cards, or physical keys, FIDO authentication ensures cryptographic security without exposing sensitive credentials. Comparative analysis shows that FIDO-based authentication provides higher security and usability, though initial adoption costs may be higher. The system was tested in a simulated environment, demonstrating faster authentication times and reduced vulnerability to cyber threats. Table 5 offers the comparison of FIDO with traditional methods.

Table 5: Comparison of FIDO-Based Authentication vs. Traditional Methods

Criteria	FIDO-Based Authentication	PIN-based Login	RFID Tag
Security	High (public-key cryptography)	Low (susceptible to brute-force attacks)	Medium (Cloning possible)
Usability	High (tap-to-login)	Medium	High
Cost	Moderate (one-time hardware cost)	Low	Low
Vulnerability	Minimal (phishing-resistant)	High (PIN can be guessed)	Medium (RFID can be duplicated)

4.1 Security Validation using AVISPA

AVISPA is an automated suite of tools for examining and validating security protocols, including network, online, and cryptographic protocols. It uses the High-Level Protocol Specification Language (HLPSL) for modeling and analysis, and the Automatic Protocol Analyzer (APPA) to identify security flaws and property

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

violations. AVISPA supports four back-ends: On-the-fly Model-Checker (OFMC), Constraint-Logic-based Attack Searcher (CL-AtSe), SAT-based Model-Checker (SATMC), and TA4SP (Tree Automata based on Automatic Approximations for the Analysis of Security Protocols).AVISPA also evaluates and creates counterexamples for user-specified security attributes, helping identify weaknesses and establishing suitable remedies. It is frequently used by the research community for formal examination of security protocols, advancing the fields of protocol architecture, security analysis methods, and creating secure communication systems. HLPSL files are used for input for AVISPA, which contains fixed-sized data blocks with unique identifications. The Dolev-Yao adversary model is used in the initial phase of the security validation procedure, specifying internet security protocols. To perform the security validation, the proposed authentication protocol is provided as input format of HLPSL to AVISPA tool and the result is obtained as SAFE in both OFMC and CL-AtSe back-end tools. Figure 3 depicts the HLPSL code for the proposed protocol. The results of AVISPA's backend tools OFMC and CL-Atse are presented in figure 4 and 5.

Registration phase	**Login and Authentication phase**

role Registration(U, A, RP)
played_by U
 	
def=
local
PK_U: public_key, SK_U: private_key,
N1: random, Signature: hash;
 	
init
step1. U -> RP : "Registration Request";
step2. RP -> U : N1;
step3. U -> A : "Generate Key Pair";
step4. A -> U : {PK_U, Sign(SK_U, N1)};
step5. U -> RP : {PK_U, Sign(SK_U, N1)};
step6. RP -> U : "Registration Success";
 	
end role.
	role Authentication(U, A, RP)
	played_by U
	
	def=
	local
	PK_U: public_key, SK_U: private_key,
	N2: random, Signature: hash;
	
	init
	step1. U -> RP : "Authentication Request";
	step2. RP -> U : N2;
	step3. U -> A : N2;
	step4. A -> U : Sign(SK_U, N2);
	step5. U -> RP : Sign(SK_U, N2);
	step6. RP -> U : "Authentication Success";
	
	end role.

Environment and Goals	**Security Goals**

environment E_Bike_Auth
def=
role_reg User, Authenticator, RelyingParty;
init
create Registration(U, A, RP);
create Authentication(U, A, RP);
end environment.
	goal
	secrecy_of SK_U;
	authentication_on N2;
	weak_authentication_of RP;

Fig. 3. HLPSL code

Fig. 4. AVISPA result OFMC backend tool

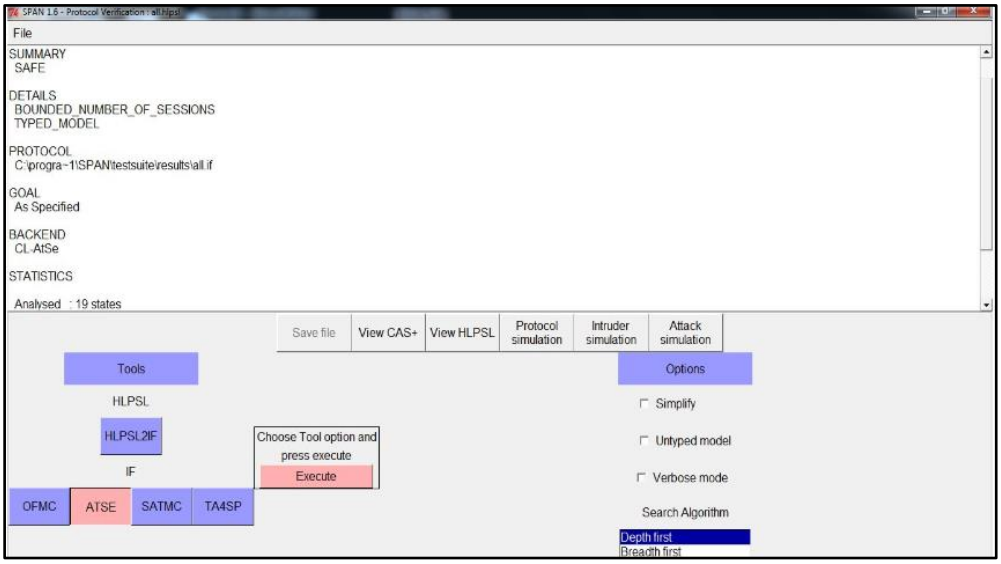

Fig. 5. AVISPA result CL-Atse too

4.2 Security analysis and attack mitigation of proposed system

The FIDO-based passwordless authentication system for e-bikes uses origin-bound authentication, secure hardware storage, and asymmetric cryptography to provide strong protection against a range of online threats. Through nonce-based challenge-response methods, it successfully counteracts replay attacks, and TLS encryption and cryptographic signatures guard against phishing and MITM assaults. Impersonation, brute-force, and stolen credential attacks are prevented since private keys never leave the FIDO authenticator. Because authentication is tied to secure enclaves (TPM, SE) and, optionally, biometric verification, the system is impervious to device theft and cloning. Insider threats, DoS assaults, and illegal access are prevented by rate-limiting, encrypted logging, and role-based access control (RBAC). Because FIDO authenticators guarantee session security, malware-based attacks and session hijacking are not feasible. All things considered, the authentication framework offers an extremely safe, intuitive, and robust way to access e-bikes, guaranteeing confidentiality, integrity, and authentication security while getting rid of password weaknesses. The summary table is provided in table 6.

Table 6: Summary of security analysis and attack mitigation

Attack Type	**Threat Description**	**Mitigation Strategy**	**Security Properties Ensured**
Replay Attack	For gaining access, attacker reuses already captured authentication message.	- Unique nonces (N_1, N_2) in each authentication request. - Used challenges are stored in server to prevent reuse. - TLS encryption prevents interception.	Authentication, Integrity, Confidentiality
Man-in-the-Middle (MITM) Attack	Authentication message is intercepted and modified.	- Message confidentiality is ensured by End-to-End TLS Encryption. - Origin Binding (EID) avoids rerouting to bogus servers. - Cryptographic Signatures (Sign_SK(H($N_2 \oplus$ EID))) ensure integrity.	Integrity, Confidentiality
Phishing Attack (Fake Server Attack)	A bogus authentication server tricks users into providing authentication responses.	- FIDO2 Authenticators Only Sign Challenges from Legitimate Domains (EID). - WebAuthn API's Same-Origin Policy slabs unauthorized access.	Authentication, Confidentiality
Brute-Force Attack on Private Keys	An attacker tries to guess the private key (SK) used for authentication.	- ECDSA-256 Encryption makes key cracking computationally infeasible. - Rate-limiting & lockout mechanisms prevent multiple failed attempts.	Authentication, Confidentiality

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

		- Private keys (SK) never leave the authenticator.	
Device Theft Attack	An attacker steals a legitimate user's FIDO authenticator and tries to authenticate.	- Biometric Authentication (Fingerprint/Face ID) in FIDO Authenticators. - Authenticator Revocation Mechanism prevents lost/stolen devices from being used. - Device-Specific Key Binding: Private keys cannot be exported or cloned.	Authentication, Access Control
Malware or Rogue Software Attack	Malicious software attempts to intercept authentication operations.	- FIDO Uses Hardware Security to Prevent Malware-Based Key Extraction. - WebAuthn API Prevents Unauthorized Applications from Accessing Credentials.	Authentication, Integrity, Confidentiality

5. Conclusions And Future Work

This paper presents a FIDO2-based password less authentication system for electric bikes, significantly enhancing security, usability, and resistance to attacks. Through a real-world prototype and comparative analysis, we validated the effectiveness of this approach. Future work includes integrating this authentication system with IoT-enabled e-bike networks, exploring alternative biometric authentication mechanisms, and further optimizing cost efficiency for large-scale deployments. To prove the security correctness of the proposed protocol, it is validated suing AVISPA tool and the result is obtained as SAFE which infers strong resistance towards vulnerable attacks. In order to facilitate safe key sharing amongst family members or fleet users, future studies on FIDO-based passwordless authentication for e-bikes can investigate improved multi-user access management utilizing decentralized identity (DID) frameworks. By using blockchain-based authentication logs, tamper-proof auditing might be enhanced and harmful modifications could be avoided.

6. Declarations

6.1 Competing Interests

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

6.2 Publisher's Note

AIJR remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

[1] Anna Angelogianni, Ilias Politis, and Christos Xenakis. 2024. How many FIDO protocols are needed? Analyzing the technology, security, and compliance. ACM Comput. Surv. 56, 8, Article 214 (August 2024), 51 pages. https://doi.org/10.1145/3654661

[2] Wenxuan Xu, Zejun Yan, Qijun Zhang, and Weifa Zheng. 2024. Research on FIDO Authentication Based on IPv6. In Proceedings of the 2023 International Conference on Artificial Intelligence, Systems and Network Security (AISNS 23). Association for Computing Machinery, New York, NY, USA, 448–451.https://doi.org/10.1145/3661638.3661723

[3] Parmar, Viral, et al. "A comprehensive study on password less authentication." *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*. IEEE, 2022.

[4] H. Kim, D. Lee and J. Ryou, "User Authentication Method using FIDO based Password Management for Smart Energy Environment," *2020 International Conference on Data Mining Workshops (ICDMW)*, Sorrento, Italy, 2020, pp. 707-710

[5] Chadwick, David W., et al. "Improved identity management with verifiable credentials and fido." *IEEE Communications Standards Magazine* 3.4 (2019): 14-20.

[6] Das, Sanchari, et al. "A qualitative study on usability and acceptability of Yubico security key." *Proceedings of the 7th workshop on socio- technical aspects in security and trust*. 2018.

[7] Simon D. Fink, Lukasz Golab, S. Keshav, and Hermann de Meer. 2017. How Similar is the Usage of Electric Cars and Electric Bicycles? In Proceedings of the Eighth International Conference on Future Energy Systems (e-Energy '17). Association for Computing Machinery, New York, NY, USA, 334–340. https://doi.org/10.1145/3077839.3078464

[8] M. Morii *et al*., "Research on Integrated Authentication Using Passwordless Authentication Method," *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, Turin, Italy,

2017, pp. 682-685

[9] Hu, Kexin, and Zhenfeng Zhang. "Security analysis of an attractive online authentication standard: FIDO UAF protocol." *China Communications* 13.12 (2016): 189-198.

[10] Künnemann, Robert, and Graham Steel. "YubiSecure? Formal security analysis results for the Yubikey and YubiHSM." *Security and Trust Management: 8th International Workshop, STM 2012, Pisa, Italy, September 13-14, 2012, Revised Selected Papers 8*. Springer Berlin Heidelberg, 2013.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922