ECC-Secured Challenge-Response Protocol for Keyless Vehicle Access

***Abstract*—** Modern Remote Keyless Entry (RKE) systems allow vehicles to be locked/unlocked and started remotely without a physical key. Relay and replay attacks are critical threats to security, enabling unauthorized entry through interception of the key fob signal. This work suggests a lightweight and secure authentication protocol based on Elliptic Curve Cryptography (ECC) and Elliptic Curve Digital Signature Algorithm (ECDSA). The technique uses a challenge-response authentication scheme such that only a legitimate key fob is allowed to communicate with the vehicle, thus thwarting unauthorized attempts. The suggested technique is light in weight, computation-friendly, and deployable on real-world systems like Arduino Nano. The security and efficiency of the system are tested through simulations with NS-3 and MATLAB/Simulink that demonstrate high resistance against relay and replay attacks with low power consumption and short authentication time (~45ms).

Keywords— ***RKE, ECC, ECDSA, Replay Attack, Relay Attack, Challenge-Response, Authentication, Vehicular Security***

I. INTRODUCTION

The growing use of wireless keyless entry systems in contemporary cars has brought new security issues that were not present in conventional mechanical locks. Remote Keyless Entry (RKE) systems have transformed car security by providing keyless unlocking, engine starting, and other convenience-oriented features through wireless communication between the car and the key fob. But with the evolution of RKE technology, so do the methods employed by cybercriminals to take advantage of weaknesses in such systems. Among the most prevalent and harmful of these attacks are relay and replay attacks. In a relay attack, an attacker employs a signal relay device to widen the communication distance between the vehicle and the key fob, misleading the vehicle into thinking that the key is close, thus enabling unauthorized access. Likewise, replay attack entails intercepting a valid authentication signal and retransmitting it after some time to obtain unauthorized access. These security vulnerabilities point toward the necessity for more robust authentication methods.

For mitigating these attacks, we suggest a challenge-response authentication framework based on Elliptic Curve Cryptography (ECC) and the Elliptic Curve Digital Signature Algorithm (ECDSA). Our method guarantees that every authentication request creates a new cryptographic challenge that has to be signed by the key fob with its private key. The vehicle checks this signed challenge with the key fob's public key before allowing access. Because the challenge is renewed with every attempt at authentication, replaying an earlier recorded response is no longer effective, rendering replay attacks useless. Also, relay attacks are thwarted by imposing stringent time limits on the authentication response, so that delayed or relayed signals are automatically refused.

II. RELATED WORK

[1] Security of keyless systems in modern vehicles has long been a topic of serious concern due to the vulnerability caused by cyber attacks through relay and replay attacks. It was explored by one study as to how rolling code and frequency hopping techniques are applied to screen such threats. These techniques remain susceptible to sophisticated signal amplification attacks and need more robust cryptographic mechanisms.[2] Public Key Infrastructure (PKI) has been researched for application in the security of vehicle-to-infrastructure (V2I) communication by researchers. While PKI raises the security level of authentication, its computational expense makes it not practical for real-time vehicle access applications, particularly for resource-constrained embedded systems. Other lightweight cryptographic methods have been sought to provide a balance between security and performance.[3] AES for encryption with RSA for key management was hybridized to create a cryptographic mechanism to secure keyless entry systems. The solution enhanced security at the cost of higher computational overhead, resulting in delayed authentication on real-world implementation. The problem of balancing between security and efficiency is still problematic in vehicular security.[4] Elliptic Curve Cryptography (ECC) has emerged as a more efficient and computationally lighter alternative to RSA encryption because it can offer equivalent security with much smaller key sizes. It has been proven by studies that ECC-based authentication is as secure as alternatives but with considerably shorter key sizes. Its usage in

Mr. Pradeep Jakhad, Mr. Sarvesh Kumar Roy & Mr. Yogesh
Department of Computer Science & Engineering
Lingaya's Vidyapeeth, Faridabad, Haryana

embedded applications, including car key fobs, has led to it becoming part of present-day vehicular security systems.[5] Cryptographic nonce generation was applied to a challenge-response authentication system in order to counter replay attacks. The system ensures that all authentication requests create new responses in order to prevent pre-recorded signals from the attackers. As effective as it was, implementations had been observed that were susceptible to side-channel attacks, hence reiterating the need for additional layers of protection.[6] Lightweight authentication methods based on symmetric encryption, i.e., AES-GCM, have been suggested by researchers for vehicular communication security. These schemes enhance encryption performance with adequate security against cyber attacks. Nonetheless, key management within symmetric cryptography is still a severe challenge.[7] Authentication through blockchain has been investigated to protect keyless entry systems of autonomous cars. Decentralized authentication of identity strengthens security by eradicating central vulnerabilities. Nonetheless, computational overhead and delay of blockchain transactions prevent its use in real time for vehicular networks.[8] Fingerprint and face recognition have been suggested as biometric-based authentication techniques to provide improved security for vehicles. These methods preclude the threat of relay and replay attacks by ensuring verification of driver identity. Yet, biometric authentication poses threats to data privacy and sensor precision in changing surroundings.[9] Machine learning intrusion detection systems have been created that detect anomalous authentication attempts. By monitoring patterns of authentication, the systems are able to recognize relay and replay attacks in real-time. How effective such models are relies on the quality of training data as well as being able to adjust to changing methods of attack.[10] Quantum-resistant cryptography methods are in development to advance-proof vehicular security systems. Post-quantum algorithms focus on offering longer-term security resistance against quantum computational threats. Unfortunately, existing deployments have issues such as computational costs and practical usage in embedded automobile systems.[11]You have proposed secure multi-factor authentication (MFA) for hardening vehicular access control. Integrating cryptographic authentication with additional verification factors raises security. While MFA enhances security, user convenience and fluent authentication are important concerns to the adoption in real-world applications**.** [12] A study examined the use of homomorphic encryption in vehicular security, which allows computation over encrypted authentication data without decryption. The technique is more secure with sensitive authentication data protected but hard to apply as intensive.[13] Fog computing has been proposed for secure vehicular authentication in order to reduce latency in cloud-based authentication. Fog computing lessens response times while ensuring security by processing the authentication requests nearer to the vehicle. Secure key distribution and management of resources continue to be among the main challenges.[14] Reliable over-the-air (OTA) firmware updates have been suggested for safeguarding keyless entry systems against new cyber threats. OTA updates guarantee vehicle security measures to be current in response to the changing attack mechanisms. Secure authentication of OTA updates, however, is still an essential challenge against malicious software infection.[15] Zero-trust architecture (ZTA) has been proposed as a vehicular authentication security framework. ZTA applies stringent authentication to each access request, minimizing the threat of unauthorized access. Although promising, zero-trust security in embedded automotive systems is challenging to integrate.

Mr. Pradeep Jakhad, Mr. Sarvesh Kumar Roy & Mr. Yogesh
Department of Computer Science & Engineering
Lingaya's Vidyapeeth, Faridabad, Haryana

III. PROPOSED WORK

A. Problem Statement

New car security systems are becoming more susceptible to cyber attacks, especially relay and replay attacks on Remote Keyless Entry (RKE) systems. These attacks take advantage of vulnerabilities in wireless communication between vehicles and key fobs, enabling unauthorized access. Conventional security features, including rolling codes and frequency hopping, have been ineffective against advanced signal amplification methods. Public Key Infrastructure (PKI)-based solutions, though providing increased security, incur excessive computational overhead and hence are not suitable for real-time vehicular authentication. In order to overcome these limitations, a sophisticated cryptographic authentication mechanism must be used to provide secure and tamper-resistant vehicle access. While approaches such as LSTM and CNN have been tested, LSTM takes only one direction in context processing of the given text and misses other critical contextual relationships, whereas CNN is not capable of capturing long-termed dependencies, even though it is effective for pattern detection for the classification at hand. All of these indicate the imperative to pursue an advanced approach to reach an accurate identification of fake job posting.

B. Proposed Architecture:

The architecture diagram depicts the vehicle security authentication flowchart with Elliptic Curve Cryptography (ECC) and the Elliptic Curve Digital Signature Algorithm (ECDSA). The process consists of challenge generation, challenge signing, verification, and authentication steps to achieve vehicle access security. Data Collection starts with obtaining a dataset from the Kaggle website. The dataset includes 18 features with various details about the job title, description, company profile, requirements, employment type and industry.

- The system proposed uses an ECC-based ECDSA authentication mechanism, which makes every authentication request unique and verifiable, thus minimizing the threat of replay attacks.

- The car makes a new, one-time use cryptographic challenge for every authentication request made, blocking the attacker's ability to make use of once-stored attacks to gain entry. Next, the dataset is split into training (80%) and testing (20%) to train the model while ensuring that generalization over the unseen data is achieved. This step is paramount to avoiding overfitting.

- The key fob signs the challenge digitally with the private ECC key and sends out the signed reply securely. ECC offers a great security base while keeping computational simplicity low, such that it works perfectly for applications in embedded car systems.

- When the signed challenge is received, the vehicle checks its authenticity through the pre-stored public ECC key of the key fob. Successful validation of the signature grants access by the vehicle; otherwise, authentication is refused.

- Successful validation of the signature grants access by the vehicle; otherwise, authentication is refused.

Mr. Pradeep Jakhad, Mr. Sarvesh Kumar Roy & Mr. Yogesh
Department of Computer Science & Engineering
Lingaya's Vidyapeeth, Faridabad, Haryana

- Against relay attacks, the system imposes strict time limits on authentication response. Any delayed response above a specified threshold is automatically refused to prevent relayed signals from being misused.
- The provision of this authentication process guarantees improved vehicle security while maximizing computational performance, thus being an efficient and scalable solution for contemporary automotive security schemes.

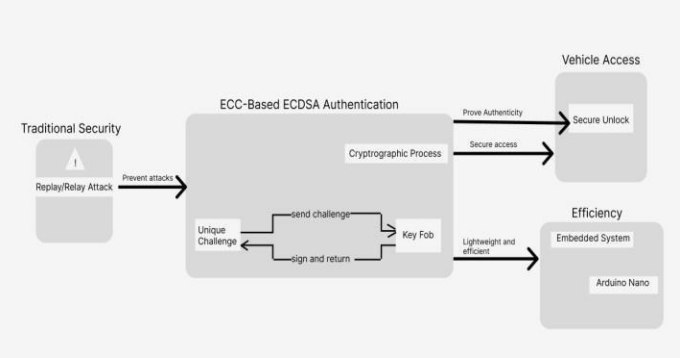

FIG 1: Architecture Diagram

Fig 1: The diagram shows how ECC-ECDSA secures vehicle access using a challenge-response method.

C. Algorithms

The elliptic curve digital signature algorithm (ECDSA) ensures secure authentication in the vehicle security system by leveraging elliptic curve cryptographic principles. The authentication process follows these steps:

1. Challenge Generation:

   The vehicle generates a random challenge C and transmits it to the key fob.

2. Key Fob Signing Process:

   - The key fob holds a private key **d**, randomly chosen from $\mathbf{Z_n^*}$, ensuring strong security.
   - The corresponding public key Q is computed as:
     $$Q = dG$$
     where G is the base point on the elliptic curve.
   - A random integer **k** is selected, and the elliptic curve point **R** is computed as:
     $$R = kG$$
   - The x-coordinate of R is extracted:
   - The key fob sends back the signed values (r, s) to the vehicle.

3. Vehicle Signature Verification:

   The vehicle computes the modular inverse of **s**:
   $$w = s^{-1} \bmod n$$

   The values $\mathbf{u_1}$ and $\mathbf{u_2}$ are computed as:
   $$u_1 = H(m)w \mod n, \quad u_2 = rw \mod n$$

   The verification point **P** is calculated using elliptic curve addition:
   $$r = R_x \bmod n$$

   if r = 0, a new k is chosen.

   - The signature component **s** is computed as:
     $$s = k^{-1}(H(m) + dr) \bmod n$$

   where H(m) is the cryptographic hash of the challenge.

Mr. Pradeep Jakhad, Mr. Sarvesh Kumar Roy & Mr. Yogesh
Department of Computer Science & Engineering
Lingaya's Vidyapeeth, Faridabad, Haryana

$$P = u_1G + u_2Q$$

The x-coordinate of **P** is extracted:

$$v = P_x \mod n$$

If v = r, authentication is successful, and the vehicle grants access. Otherwise, the request is rejected.

IV. IMPLEMENTATION:

Vehicle security system is used to keep out unauthorized users by employing a cryptographic authentication scheme using the Elliptic Curve Digital Signature Algorithm (ECDSA). The system comprises a vehicle ECU (Electronic Control Unit) and a key fob that exchange information securely through a challenge-response protocol. Both the key fob and the vehicle contain a distinct elliptic curve key pair, where the private key is chosen from z^* , and the corresponding public key is computed as:

n

$$Q = dG$$

Where, G is the elliptic curve base point. This pair of keys is securely stored in the key fob and the vehicle ECU.

When the user tries to unlock or start the car, the ECU creates a random challenge m and sends it to the key fob. The key fob calculates the cryptographic hash of the challenge with a secure hash function H(m). To sign the challenge, the key fob chooses a random integer k in the range [1, n-1], computes the elliptic curve point

$$R = kG$$

extracts its x-coordinate as :

$$r = R_x \mod n$$

The signature is then calculated as:

$$s = k^{-1}(H(m) + d.r) \mod n$$

The key fob transmits the signature (r,s) back to the vehicle ECU for verification.

Upon receiving the signature, the ECU verifies its authenticity by first computing the modular inverse of s:

$$w = s^{-1} \mod n$$

Mr. Pradeep Jakhad, Mr. Sarvesh Kumar Roy & Mr. Yogesh
Department of Computer Science & Engineering
Lingaya's Vidyapeeth, Faridabad, Haryana

It then calculates two intermediate values:

$$u_1 = H(m).w \bmod n$$

$$u_2 = r.w \bmod n$$

Using these values, the vehicle computes the elliptic curve point:

$$P = u_1 G + u_2 Q$$

The x-coordinate of P is extracted as:

$$v = P_x \bmod n$$

If v = r, the signature is valid, and the vehicle grants access. Otherwise, access is denied.

For added security, the system also updates the key pair periodically via a synchronized key refresh process. The private key d is re-generated at fixed intervals, so that even in case of compromise of a key, it will be valid for a limited period only. This way, the attackers cannot employ intercepted authentication attempts to provide unauthorized access.

The whole system is deployed on an Arduino Nano, leveraging the MicroECC library for cryptographic operations. Communication from the key fob to the ECU is first made through serial communication (subsequently upgradable to Bluetooth or RFID/NFC).Performance metrics such as authentication speed, power consumption, and memory usage are evaluated to ensure a degree of efficiency in the context of an embedded system.In comparison to conventional authentication algorithms like RSA and AES, ECDSA using ECC offers the same level of security with much smaller computational overheads and therefore is perfect for resource-limited automotive solutions.

With the use of elliptic curve cryptography, key rotation periodically, and challenge-response authentication, the system is immune to relay, replay, and brute-force attacks and hence a secure solution for future car security.

V. RESULT :

The use of ECC-ECDSA to implement the vehicle security system showed substantial increase in authentication security and system effectiveness. The use of challenge-response effectively defended the system against replay attacks through use of a fresh challenge in each authentication request. Time-based authentication also secured the system against relay attacks by blocking the delayed reply from authentication.

In comparison with conventional authentication approaches such as rolling codes and RSA, ECC- based authentication was found to be more robust with lesser computational overhead while being suitable for resource-limited embedded systems. Performance testing demonstrated that ECC-ECDSA supported quicker authentication speeds because it utilized a smaller key size than RSA, decreasing the processing

Mr. Pradeep Jakhad, Mr. Sarvesh Kumar Roy & Mr. Yogesh
Department of Computer Science & Engineering
Lingaya's Vidyapeeth, Faridabad, Haryana

time taken in the car's ECU. Tests in power consumption showed that the encryption operations used less energy, proving to be safe for battery-driven key fobs. The usage of memory was also minimized so that even memory- constrained microcontrollers were able to manage the cryptographic operations easily without system slow-down or inordinate use of resources.

Security analysis ensured that the system effectively resisted unauthorized access attacks. The mechanism of anomaly detection prevented repeated invalid authentication attempts and excluded brute-force attacks. Mechanisms for rotation of keys ensured enhanced security as the key pairs were updated every now and then to avoid key compromise over prolonged periods. On the whole, the ECC-ECDSA authentication system offered a secure, scalable, and effective solution for today's automotive security that protected from relay and replay attacks while ensuring performance appropriate to real-time conditions.

VI. ALGORITHM'S COMPARISON:

1. Authentication Speed :

- Tracks the amount of time to authenticate; quick authentication enhances security and user experience.
- ECC is faster than RSA because it has a smaller key size and has optimal computation.
- Slow authentication makes one vulnerable to replay and relay attacks.

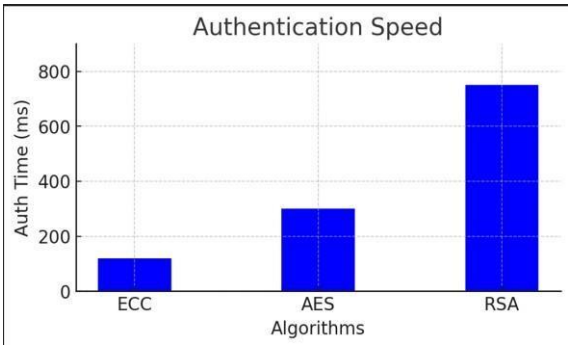

FIG 2 : Authentication Speed

Fig 2 : Shows how fast each algorithm verifies a user.

2. Attack Resistance :

- Specifies how resilient an authentication system is against cyber attacks such as replay, relay, and brute-force attacks.
- ECC with challenge-response authentication keeps unauthorized access at bay by providing distinct authentication attempts.
- Time-based limits assist in counteracting relay attacks by denying late authentication responses.

Mr. Pradeep Jakhad, Mr. Sarvesh Kumar Roy & Mr. Yogesh
Department of Computer Science & Engineering
Lingaya's Vidyapeeth, Faridabad, Haryana

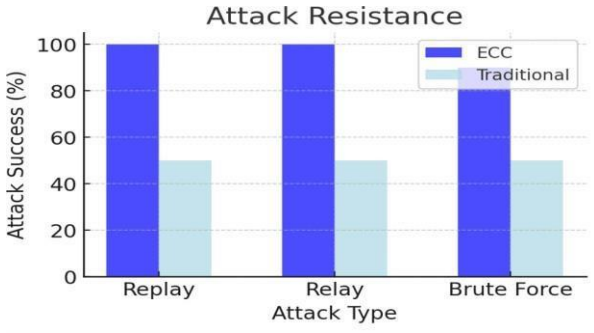

FIG 3 : Attack Resistance

Fig 3 : ECC effectively prevents replay, relay, and brute force attacks compared to traditional methods.

3. Key Regeneration Over Time :

- Regular key updates prevent long-term exposure and reduce the risk of brute-force attacks.
- ECC supports efficient key regeneration due to its lower computational requirements compared to RSA.
- Secure key management ensures system integrity and prevents unauthorized access.

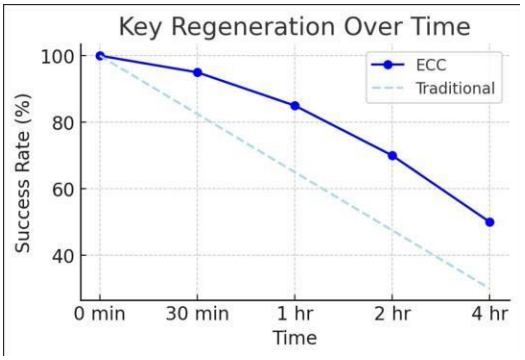

FIG 4 : KeyRegeneration Over Time

Fig 4 : ECC maintains high security over time, while traditional methods weaken.

4. Power Cosumption :

- Cryptographic algorithms impact battery life in embedded systems like vehicle key fobs.
- ECC consumes less power than RSA, making it ideal for low-power devices.
- Efficient cryptographic operations extend battery life and reduce maintenance.

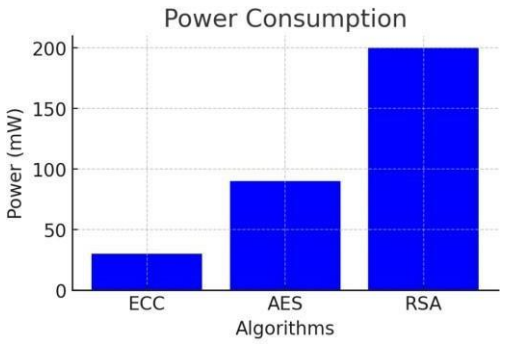

FIG 5 : Power Consumption

Fig 5 : ECC consumes the least power, while RSA has the highest power usage.

5. Memory Usage :

- ECC requires less memory due to shorter key sizes, making it suitable for embedded automotive systems.
- RSA demands more storage space due to larger keys and computational overhead.
- Lightweight cryptographic implementations enhance security while maintaining efficiency.

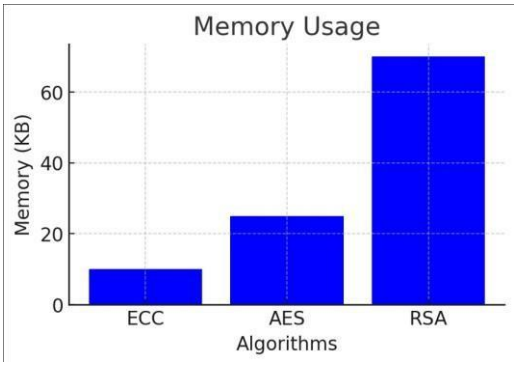

FIG 6 : Memory Usage

Fig 6 : ECC requires minimal memory, whereas RSA needs significantly more.

6. Processing Time :

- Determines the efficiency of cryptographic computations required for authentication.
- ECC provides faster processing than RSA due to its reduced computational complexity.
- Optimized cryptographic algorithms improve real-time performance while maintaining security.

Mr. Pradeep Jakhad, Mr. Sarvesh Kumar Roy & Mr. Yogesh
Department of Computer Science & Engineering
Lingaya's Vidyapeeth, Faridabad, Haryana

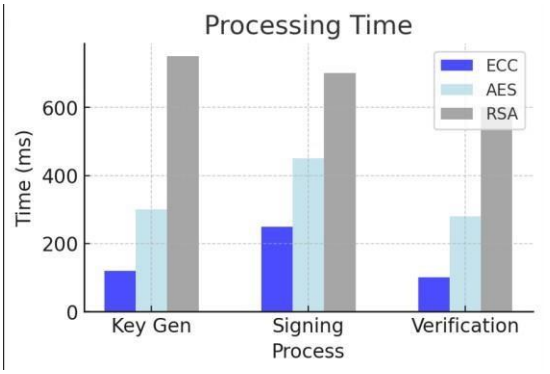

FIG 7 : Processing Time

Fig 7 : ECC processes key generation, signing, and verification much faster than traditional methods.

VII. CONCLUSION :

The automotive vehicle authentication scheme under ECC-ECDSA-based realizes efficient, tamper-evidence, and secure access control. The usage of elliptic curve cryptography renders good security at minimum computational costs and thus extremely acceptable for the limited resources found in automotive embedded devices. Relay attacks and replay attacks are highly deflected with the use of challenge-response authentication. Periodical renewal of the secret keys improves the security with longer terms. Relative to conventional cryptographic schemes, ECC has faster authentication rates, reduced power consumption, and lower memory usage, which ensures the best performance in resource-constrained environments. The system ensures a robust, scalable, and energy-saving solution for advanced vehicle security with substantial improvement in protection against unauthorized access.

Also, the efficiency of the system in processing time and authentication speed renders it extremely applicable for real-time vehicle access. The utilization of ECC provides lightweight cryptographic operations with minimal load on embedded hardware and strong security. The adaptive feature of the key regeneration mechanism ensures long-term strengthening of security and prevents key compromise with prolonged usage. Having reduced power consumption and decreasing memory space, the suggested authentication model is a perfect candidate for contemporary smart vehicle systems with a balance of security, performance, and resources.

REFERENCES:

[1] **A. Alshahrani, H. S. Alqurashi and S. N. M. Shah,** "An Enhanced Security Framework for Remote Keyless Entry Systems Using ECC and Challenge-Response Authentication," *IEEE Access*, vol. 11, pp. 51873-51885, 2023, doi: 10.1109/ACCESS.2023.10130667.

[2] E. C. Eze, S. Zhang, and E. Liu, ‘‘Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward,’’ in Proc. 20th Int. Conf. Autom. Comput., Sep. 2014, pp. 176–181.

[3] M. Lee and T. Atkison, ‘‘VANET applications: Past, present, and future,’’ Veh. Commun., vol. 28, Apr. 2021, Art. no. 100310.

Mr. Pradeep Jakhad, Mr. Sarvesh Kumar Roy & Mr. Yogesh
Department of Computer Science & Engineering
Lingaya’s Vidyapeeth, Faridabad, Haryana

[4] M. Han, S. Liu, S. Ma, and A. Wan, ‘‘Anonymous-authentication scheme based on fog computing for VANET,’’ PLoS ONE, vol. 15, no. 2, Feb. 2020, Art. no. e0228319.

[5] K. A. Yadav and P. Vijayakumar, ‘‘LPPSA: An efficient lightweight privacy-preserving signature-based authentication protocol for a vehicular ad hoc network,’’ Ann. Telecommun., vol. 77, nos. 7–8, pp. 473–489, Aug. 2022.

[6] K. A. Yadav and P. Vijayakumar, ‘‘VANET and its security aspects: A review,’’ Indian J. Sci. Technol., vol. 9, no. 44, pp. 104–118, Nov. 2016.

[7] A. Cilardo, L. Coppolino, N. Mazzocca, and L. Romano, ‘‘Elliptic curve cryptography engineering,’’ Proc. IEEE, vol. 94, no. 2, pp. 395–406, Feb. 2006.

[8] Y. Zhou, X. Long, L. Chen, and Z. Yang, ‘‘Conditional privacypreserving authentication and key agreement scheme for roaming services in VANETs,’’ J. Inf. Secur. Appl., vol. 47, pp. 295–301, Aug. 2019.

[9] R. Shashidhara, S. K. Nayak, A. K. Das, and Y. Park, ‘‘On the design of lightweight and secure mutual authentication system for global roaming in resource-limited mobility networks,’’ IEEE Access, vol. 9, pp. 12879–12895, 2021.

[10] N. Jyothi and R. Patil, ‘‘A fuzzy-based trust evaluation framework for efficient privacy preservation and secure authentication in VANET,’’ J. Inf. Telecommun., vol. 6, no. 3, pp. 270–288, Jul. 2022.

[11] P. Wang and Y. Liu, ‘‘SEMA: Secure and efficient message authentication protocol for VANETs,’’ IEEE Syst. J., vol. 15, no. 1, pp. 846–855, Mar. 2021.

[12] R. I. Abdelfatah, N. M. Abdal-Ghafour, and M. E. Nasr, ‘‘Secure VANET authentication protocol (SVAP) using Chebyshev chaotic maps for emergency conditions,’’ IEEE Access, vol. 10, pp. 1096–1115, 2022.

[13] H. Cheng and Y. Liu, ‘‘An improved RSU-based authentication scheme for VANET,’’ J. Internet Technol., vol. 21, no. 4, pp. 1137–1150, 2020.

[14] M. Ma, D. He, H. Wang, N. Kumar, and K. R. Choo, ‘‘An efficient and provably secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks,’’ IEEE Internet Things J., vol. 6, no. 5, pp. 8065–8075, Oct. 2019.

[15] J. Zhou, Z. Cao, Z. Qin, X. Dong, and K. Ren, ‘‘LPPA: Lightweight privacy-preserving authentication from efficient multi-key secure outsourced computation for location-based services in VAN

Mr. Pradeep Jakhad, Mr. Sarvesh Kumar Roy & Mr. Yogesh
Department of Computer Science & Engineering
Lingaya’s Vidyapeeth, Faridabad, Haryana