Performance Evaluation of Biometric Fingerprint Orientation in IoT-Enabled Motorcycle Security Systems with GPS Tracking

Muzalifah Mohd Said[1], M. Afiq Aizat Mustafa[1,2], Siti Aisah Mat Junos[1], Faiz Arith[1], Hafzaliza Erny Zainal Abidin[3]

[1]Faculty of Electronics and Computer Technology and Engineering, University Technical Malaysia Melaka (UTeM), Melaka, Malaysia.

[2]China State Construction Engineering, Jalan Strachan Off Jalan Sultan Azlan Shah, Kuala Lumpur, Malaysia.

[3]Institute of Microengineering and Nanoelctronics, University Kebangsaan Malaysia, Selangor, Malaysia.

DOI: https://dx.doi.org/10.47772/IJRISS.2025.909000716

Received: 20 September 2025; Accepted: 26 September 2025; Published: 28 October 2025

ABSTRACT

Motorcycle theft continues to pose significant challenges despite widespread use of conventional locks and alarms, highlighting the limitations of traditional security systems. Recent research has explored biometric authentication, IoT-based monitoring, and GPS-enabled tracking as potential solutions, yet most studies address these technologies in isolation. This leaves a critical gap in understanding how their integration can enhance both reliability and usability in real-world conditions. By analyzing the intricate patterns of a rider's fingerprint ridges, this system offers unparalleled user identification and authentication, granting access only to authorized individuals. The integrated GPS tracker provides real-time location monitoring, enhancing security and offering invaluable assistance in case of theft. Leveraging the power of IoT technology, the system seamlessly transmits data between components, ensuring efficient operation and remote monitoring. This project has the potential to revolutionize motorcycle security, reducing theft rates, boosting rider safety, and paving the way for future advancements in vehicle security solutions.

Keywords—Motorcycle System, IoT Technology, Biometric Security, GPS tracker, Fingerprint

INTRODUCTION

The transportation industry has experienced a transformation thanks to the incorporation of modern technology like GPS monitoring, biometric authentication, and the Internet of Things (IoT). The application of high-tech systems to improve the security, safety, and riding experience of motorbikes has gained more attention in recent years [1-4]. In order to investigate the use of biometric fingerprint orientation as a safe technique for motorcycle identification and control, the project "Analysis on Biometric Fingerprint Orientation for Hi-Tech Motorcycle System Using IoT Technology with GPS Tracker" was created.

Motorcycle theft is a common problem that creates major challenges for both individual motorcyclists and the larger community. Despite the use of standard anti-theft devices like locks and alarms, motorcycles are still a target for theft due to their mobility and simplicity of disassembly [5]. Unsuitable fingerprint technology is another problem that arises when it comes to biometric fingerprint orientation. The dependability of a security system's technological components determines how successful it is [6]. Problems including fingerprint identification errors, environmental sensitivity, and ease of usage become important considerations when it comes to biometric fingerprint orientation [7-9]. Real-time location information is also essential for theft prevention and efficient tracking mechanisms.

Numerous studies and existing systems have explored the integration of biometrics, IoT and GPS technology in different domains. Some research focuses on biometric- based access control systems, highlighting the

accuracy and efficiency of fingerprint recognition techniques. Others examine IoT-enabled motorcycle systems, emphasizing remote control, real-time monitoring, and data analytics capabilities. Several projects have explored the use of GPS tracking in motorcycles to improve security and recovery mechanisms. However, a comprehensive analysis specifically targeting the combination of biometric fingerprint orientation, IoT technology, and GPS tracking in hi-tech motorcycle systems is limited [10,11].

The research aims to integrate fingerprint orientation with existing IoT infrastructure and GPS tracking systems to create a reliable and efficient motorcycle system. A prototype is developed and extensive tested to access reliability, accuracy, and IoT technology in the motorcycle industry, offering insights for improved rider safety, theft prevention, and efficient tracking mechanisms. The potential commercialization of the hi-tech motorcycle system utilizing IoT technology with GPS tracker and biometric fingerprint orientation is significant, offering enhanced security features, convenient access control, and efficient tracking mechanisms for various industries.

METHODOLOGY

A. Initialize Hardware Components

To set up a fingerprint sensor and GPS, connect them to a microcontroller or development board and configure their communication by adjusting protocols, baud rate, data format and parameters. Once initialized, the modules collaborate to perform functions such as sending GPS location data and conducting fingerprint authentication. For this project, capacitive fingerprint R-503 and NEO-6M GPS module are being used. The components are shown in Fig. 1 and Fig. 2 below:

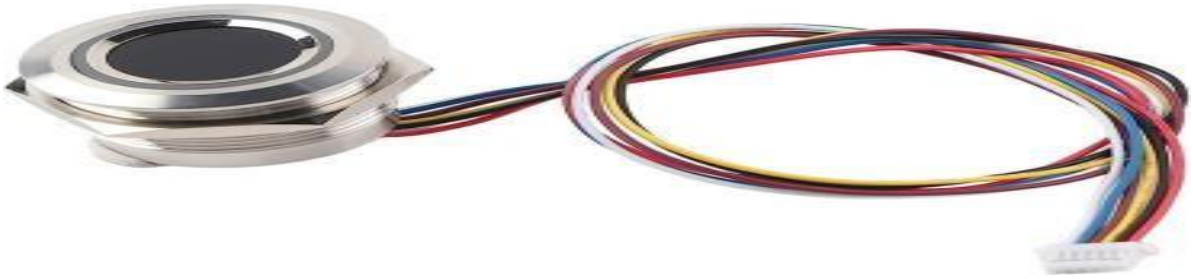

Figure 1: Capacitive Fingerprint R-503

Figure 2: NEO-6M GPS Module

B. Biometric Fingerprint Detection

When the motorcycle switch is turned on, the circuit activates and initializes the fingerprint sensor. The user scans their fingerprint for motor activation [13-15]. In this project, the fingerprint orientation analysis relies primarily on minutiae extraction, where ridge endings and bifurcations are identified from the captured image. Orientation fields are computed to represent the local ridge flow, allowing the system to distinguish between different fingerprint patterns such as arches, loops, and whorls. This approach improves robustness in matching, as orientation features remain stable even under partial or low-quality impressions. The matching

algorithm applies a hybrid strategy combining minutiae-based matching with ridge orientation correlation, ensuring both accuracy and resilience against noise or distortions.

C. Initializing IoT Function

The GPS sensor activates when the user rides the motorcycle, sending location info to the smartphone app. Before that, the user will be notified if the motorcycle is start and if there are any false fingerprint attempts as shown in Fig. 3 below:

Figure 3: Notification of Alert

D. IoT Observation and Control

Recent empirical studies underscore this shift, emphasized the importance of integrating GPS and GSM modules for real-time monitoring, showing significant improvements in theft recovery but also raising questions about data reliability and user accessibility. These findings suggest that while IoT and biometric solutions are promising, their effectiveness depends on addressing technical reliability, environmental sensitivity, and user trust.

The Blynk app displays the location data for the user and allows control over the motor ignition. In Fig. 4, it shows how the display on Blynk app where the control button for ON/OFF, speed indicator and maps for location of motorcycle. Beyond hardware security, the IoT ecosystem of the motorcycle requires protection of data transmitted between the GPS module, microcontroller, and the Blynk smartphone application. Without proper safeguards, this communication may be susceptible to eavesdropping, spoofing, or man-in-the-middle attacks.

To mitigate these risks, secure protocols such as AES-128 encryption and TLS-based communication channels can be implemented, ensuring confidentiality and integrity of the data. Additionally, device-level authentication using unique tokens or digital certificates further prevents unauthorized access, enhancing the overall resilience of the system.

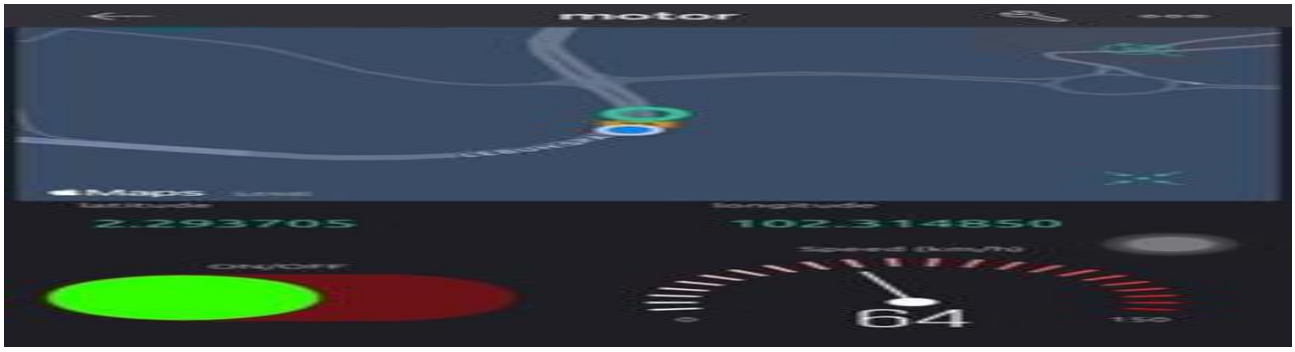

Figure 4: Display of Blink Apps

E. Accuracy of GPS Location

Regarding the accuracy of GPS location, numerous steps have been taken to measure its precision through the following procedures:

1. Set up NEO-6M in a clear sky location with minimum signal obstruction.
2. Record its position data for a predetermined duration (e.g., 30 minutes, 1 hour).
3. Compare the recorded position with a reference location known with high accuracy
4. Calculate metrics like mean error, root mean square error (RMSE) and maximum error to access positional accuracy
5. Compare the data with the actual route using software like Google Maps.

F. Formula

To calculate mean error, root mean square error and maximum error that related to this project, some formulas I need to be used [14]:

i. Mean Error

Calculate the average difference between the GPS- measured positions and the reference positions in each coordinate (latitude, longitude, altitude) by using formula (1).

$$Mean\ Error = \frac{\sum(measured\ position - Reference\ Position)}{Number\ of\ Samples} \text{ ...(1)}$$

ii. Root Mean Square Error (RMSE)

Provides a more comprehensive measure of error by accounting for both positive and negative deviations, formula (2) being used to calculate RMSE.

$$RMSE = \sqrt{\frac{\sum(measured\ position - Reference\ Position)^2}{Number\ of\ Samples}} \text{ ... (2)}$$

iii. Maximum Error

Indicates the largest deviation observed in any single measurement. Formula (3) been used in order to calculate maximum error.

$$Maximum\ Error = Max(|Measured\ Position - Reference\ Position|) \text{ ...(3)}$$

G. Fingerprint Data

The collected fingerprint data is under analysis to gauge its accuracy by assessing two crucial metrics, namely FAR (False Acceptance Rate) and FRR (False Rejection Rate). A total of 127 fingerprints with 2 impressions have been gathered for this analysis, with the following procedures:

Collecting Data

1. Genuine Fingerprints: Capture high-quality fingerprint images or feature vectors from authorized users (hundreds or thousands for statistically significant results).

2. Imposter Fingerprints: Collect samples from unauthorized individuals (smaller set proportional to genuine users).

System Setup and Configuration

1. Connect the R503 sensor and ensure proper communication with the software.
2. Enroll genuine users by capturing and storing their fingerprint templates in the system.

Conduct Testing

1. Have all genuine users attempt to access the system using their fingerprints. Record these as genuine attempts.
2. Have all imposter individuals attempt to bypass the system with their own or someone else's fingerprints. Record these as imposter attempts.
3. For each attempt, classify it as a correct match, false accept (imposter accepted), or false reject (genuine user rejected).

Calculate FAR, FRR and EER

1. Calculate FAR as shown in formula (4), as the percentage of imposter attempts resulting in false matches (accepted) divided by the total number of imposter attempts [16].
2. Calculate FRR with using formula (5) as the percentage of genuine attempts resulting in false non-matches (rejected) divided by the total number of genuine attempts.
3. Calculate EER by using the formula (6).

$$FAR = \left(\frac{Number\ of\ False\ Positive\ Matches}{Number\ of\ Imposter\ Attempts}\right) \times 100\% \text{ …..(4)}$$

$$FRR = \left(\frac{Number\ of\ False\ Negative\ Matches}{Number\ of\ Genuine\ Attempts}\right) \times 100\% \text{ ….(5)}$$

$$EER = \left(\frac{FAR+FRR}{2}\right) \text{ ……(6)}$$

RESULT AND ANALYSIS

Latitude and Longitude Data

The Blynk app not only displays the current location of the motorcycle but also provides speed data for analysis. Data collection occurs within a defined time frame, specifically 1 minute, resulting in a total of 20 samples, with the reference position set at (2.289476, 102.304875)). The GPS pinpoint, alongside constant latitude and longitude values, remains static for fixed positioning. However, a slight volatility is observed, with latitude and longitude values fluctuating within a range of approximately +-0.000029, characterized as the Maximum Error, which does not impact the positioning. The Mean Error, calculated for each latitude and longitude based on Table 1 below, yields values of - 0.0000001 for latitude and -0.0000023 for longitude. As for the Root Mean Square Error (RMSE), the obtained values are 0.000016 for both latitude and longitude.

Table 1: Collected Latitude and Longitude Data

Reference Position = (2.289476, 102.304875)						
No.	**Latitude**	**Latitude Difference**	**Difference ^2**	**Longitude**	**Longitude Difference**	**Difference ^2**
1	2.289455	-0.000021	4.41E-10	102.304899	0.000024	5.76E-10

2	2.289493	0.000017	2.89E-10	102.304846	-0.000029	8.41E-10
3	2.289505	0.000029	8.41E-10	102.304885	0.000010	1.00E-10
4	2.28945	-0.000026	6.76E-10	102.304862	-0.000013	1.69E-10
5	2.289479	0.000003	9.00E-12	102.304895	0.000020	4.00E-10
6	2.289468	-0.000008	6.40E-11	102.304863	-0.000012	1.44E-10
7	2.289495	0.000019	3.61E-10	102.304861	-0.000014	1.96E-10
8	2.289459	-0.000017	2.89E-10	102.304855	-0.000020	4.00E-10
9	2.289486	0.000010	1.00E-10	102.304891	0.000016	2.56E-10
10	2.289462	-0.000014	1.96E-10	102.304858	-0.000017	2.89E-10
11	2.289481	0.000005	2.50E-11	102.304864	-0.000011	1.21E-10
12	2.289452	-0.000024	5.76E-10	102.304888	0.000013	1.69E-10
13	2.289497	0.000021	4.41E-10	102.304879	0.000004	1.60E-11
14	2.289465	-0.000011	1.21E-10	102.304881	0.000006	3.60E-11
15	2.289489	0.000013	1.69E-10	102.304869	-0.000006	3.60E-11
16	2.289471	-0.000005	2.50E-11	102.304852	-0.000023	5.29E-10
17	2.289492	0.000016	2.56E-10	102.30487	-0.000005	2.50E-11
18	2.289461	-0.000015	2.25E-10	102.304892	0.000017	2.89E-10
19	2.289484	0.000008	6.40E-11	102.304857	-0.000018	3.24E-10
20	2.289474	-0.000002	4.00E-12	102.304887	0.000012	1.44E-10
Total Sum $\sum$		**-0.000002**	**5.17E-09**		**-0.000046**	**5.06E-09**

Upon examining the Blynk interface, disparities in location pinpoint accuracy are evident. Despite this, copying the longitude and latitude numbers from the Blynk app into mapping services like Google Maps allows for precise identification of the motorcycle, even if the displayed position may not be entirely accurate. This suggests that while the Blynk interface may have presentation shortcomings, the underlying GPS data proves dependable and can be verified using third-party mapping applications.

The GPS sensor boasts a commendable accuracy of 95%, providing exact latitude and longitude values and establishing itself as a reliable device. However, the pinpoint location feature in the Blynk app exhibits real-time errors, resulting in a 25% reduction in accuracy based on the formula used.

Although the GPS module provides reliable latitude and longitude values, the Blynk application occasionally exhibits positional discrepancies. This disparity is likely due to limited refresh rates, data buffering within the Blynk server, or constraints in the embedded mapping API. One potential solution is to optimize the data sampling interval to reduce latency while applying filtering techniques such as the Kalman filter to smooth out transient fluctuations. Alternatively, integrating the system with advanced mapping services like Google Maps API or Mapbox, which are designed for real-time navigation, could significantly improve pinpoint accuracy and reduce user-reported errors.

Power Consumption

In fingerprint sensor technology, two main types dominate: capacitive and optical. Both offer distinct advantages and drawbacks, and one key differentiating factor is power consumption. This analysis delves into the power consumption profiles of two specific models: the capacitive R503 and the optical AS608.

As depicted in Table 2, a clear distinction in power consumption emerges among various sensors. While the voltage readings exhibit marginal differences between the AS608 and R503 sensors, significant variations become evident in the current consumption during both idle and scanning phases. Specifically, the AS608 sensor draws more current than the R503 sensor during idle and scanning, with the scanning phase witnessing a notable increase in the R503 current flow.

The dissimilarity in power consumption can be attributed to the active nature of optical sensors like the AS608. These sensors emit light, typically from an LED, to illuminate the fingertip and capture its image using a CMOS sensor. Even in the absence of a finger, the LED maintains a low-power glow for readiness, contributing to a higher baseline power consumption. The constant low-level activity, including ongoing image processing by the microcontroller during idle periods, further contributes to the baseline power consumption. During fingerprint scanning, the sensor focuses its resources on the specific area covered by the finger, reducing power consumption compared to full-area monitoring in the idle state.

Conversely, capacitive sensors operate passively, relying on changes in the electric field caused by a finger's presence to detect details. In the absence of a finger, the electric field remains stable, resulting in minimal power consumption during idle periods. The sensor requires no processing when no finger is present, leading to near-zero power consumption in the idle state. However, during the scanning period, the capacitive sensor continuously scans the entire sensing area, even in the absence of a finger, contributing to a higher baseline power consumption compared to the idle state.

Table 2: Power Consumption of Fingerprint Sensor

Sensor	Voltage (V)	Current (mA) (Idle)	Current (mA) (Scanning Finger)
R503 (capacitive)	3.304	13.93	20.64
AS608 (optical)	3.296	63.1	2.85

FAR, FRR and EER Analysis

To facilitate the analysis, a total of 200 attempts were made carefully using imposter fingerprints to subject the fingerprint sensor to scanning, aiming to measure the False Acceptance Rate (FAR). Following this, the identical steps were iterated using genuine fingerprints to assess the False Rejection Rate (FRR).

Upon analyzing the results, it was observed that, following all attempts, the False Rejection Rate (FRR) exceeded the False Acceptance Rate (FAR). The FAR value stood at 0%, indicating that no imposter successfully gained access. Out of the 200 attempts, there were 4 instances of genuine match fingerprints being rejected, resulting in an FRR value of 2%.

Consequently, the acquired data reveals a False Acceptance Rate (FAR) of 0% and a False Rejection Rate (FRR) of 2%, appearing to be relatively low figures. A diminished FAR and FRR imply a high level of precision and accuracy in the sensor's image processing for individual fingerprints. These lower rates also contribute to a reduced Equal Error Rate (EER) which is of 1%, enhancing the reliability of the overall assessment.

CONCLUSION

The decision has been reached to use a capacitive fingerprint sensor as the main component for the motorbike security and control project, preferring for it over the optical fingerprint option, after careful investigation and assessment of numerous fingerprint recognition technologies.

The capacitive fingerprint sensor was chosen primarily because of its better performance, particularly when used with a motorcycle security system. Capacitive fingerprint sensors measure the electrical impulses

produced by fingerprint ridges and valleys using the electrical conductivity principle as their basis of operation. Compared to optical sensors, this technology has clear advantages, especially in terms of precision and dependability.

Capacitive sensors are not affected by ambient light, in contrast to optical sensors, which depend on light absorption and reflection to record fingerprint pictures. Because they are not affected by changes in outside lighting, capacitive sensors are more reliable and suited for outdoor uses, such those found in motorbike security systems. The capacitive sensor's dependability contributes to the security system's overall dependability by guaranteeing consistent and precise fingerprint identification regardless of ambient lighting.

Moreover, capacitive sensors are well-known for their capacity to record fingerprint images in high resolution, giving the fingerprint data additional fine-grained detail. This high degree of detail lowers the possibility of false positives or false negatives while improving fingerprint matching accuracy. When it comes to ensuring that only authorized users are able to access a motorcycle through a security system, accuracy is crucial, and the capacitive sensor is excellent at providing this accuracy.

The selection of a capacitive fingerprint sensor is also heavily influenced by how long-lasting and resilient it is. Motorcycles are subjected to a variety of external factors, such as dust, moisture, and temperature changes, therefore having a strong and durable fingerprint sensor is essential for long-term dependability. Compared to optical sensors, capacitive sensors provide a more robust option because they are solid-state and less prone to mechanical faults.

In summary, the capacitive fingerprint sensor was selected for the motorbike security and control project because to its exceptional accuracy, dependability in a range of lighting scenarios, high resolution for accurate fingerprint matching, and strong durability in demanding settings.

Future Enhancement

Capacitive fingerprint sensor developments in the future might take biometric authentication technology to an even higher level. Capacitive sensor integration with other types of biometric data is one potential path that could lead to multi-factor authentication systems. By combining fingerprint recognition with other biometric information, this method would strengthen security protocols and increase the difficulty of unauthorized access.

Future development of capacitive sensors is expected to bring out significant advancements in anti-spoofing methods. Capacitive sensors are expected to include increasingly complex algorithms and technology to detect and refuse various spoofing tactics as security risks advance. With this improvement, the sensor will be more resistant to attempts to deceive it using fake fingerprints or other illegal techniques.

Moreover, advances in materials science research and development could result in the production of capacitive sensors that are more durable and resilient. Future developments could incorporate advanced materials that are resistant to severe weather, which would make capacitive sensors perfect for use in a wider range of environments, such as outdoor and industrial ones.

Capacitive fingerprint sensors have a lot of interesting possibilities awaiting it. The next generation of capacitive sensors is expected to be shaped by major improvements in materials science, stronger anti-spoofing methods, improved sensor resolution, and compatibility with other biometric modalities. These developments will likely enhance the performance, security, and versatility of capacitive sensors.

The proposed system demonstrates promising potential for real-world deployment. The hardware components, including the capacitive fingerprint module and GPS tracker, are cost-effective, with an estimated implementation cost of less than USD 80 per unit in prototype form. When scaled for mass production, the cost can be further reduced through component optimization and integration. The long-term benefits include substantial reductions in motorcycle theft, potential insurance premium discounts for users, and improved peace of mind for owners. From a commercial perspective, this system can be marketed not only as an

aftermarket security upgrade but also as an OEM feature for motorcycle manufacturers, offering strong prospects for adoption in both local and international markets.

ACKNOWLEDGMENT

The authors would like to greatly express their thanks and appreciation to the Centre for Research and Innovation Management (CRIM) and University Technical Malaysia Melaka (UTeM) for their help in completing this research work.

REFERENCES

1. Jain, A. K., Ross, A., & Nandakumar, K. (2016). Introduction to biometrics. Springer.
2. P Sihombing, IS Daulay, S Efendy (2020). Motor Vehicle Security Using Microcontroller, GPS and Android as Innovation to Prevent Motor Thieves
3. B Kodavati, VK Raju, SS Rao, AV Prabu (2011). GSM and GPS based vehicle location and tracking system.
4. Vehicle Theft Reduction Council of Malaysia Berhad (VTREC). (n.d.). Statistics of the stolen vehicles in Malaysia (2021–2022). VTREC. Retrieved September 11, 2025, from https://www.vtrec.net/?page_id=455
5. G. More, A. Y. Kulal, H. S. Khemkar, and S. S. Nikam, "The fingerprint and RFID bike ignition with protective system," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 7, no. 3, 2025.
6. M. Furqan, M. Ikhsan, A. H. Hasugian, "Application of Security System of Motorcycle Used Fingerprint Optical Sensor and Vibration Sensor with Fuzzy Logic Based on Arduino Uno R3", JURNAL INFOKUM, Volume 10, No.1, December 2021.
7. S. Kayathri, J. Jusvanth Raja, A. Ishwarya, R. Gokul, and G. Chandrabose, "Bio lock license and fingerprint-enabled bike security system," *International Scientific Journal of Engineering and Management*, Apr. 23, 2025.
8. M.K. M Noor, M. M. Said, "Analyze on Fingerprint Devices for Motorcycle Starter and Tracking System Using IoT", Proceedings of Innovation and Technology Competition (INOTEK) 2021.
9. M. Situmorang, E. F. Y. Aritonang, "Designing Motorcycle Safety System Using Fingerprint Sensor, SMS Gateway, and GPS Tracker Based on ATMega328", Journal of Technomaterial Physics Vol. 3, No. 1, 2021.
10. A. Anusha, V.Triveni, "Detection and Track Vehicle Position by with GPS Module with Internet of Things", (Ijitr) International Journal of Innovative Technology and Research Volume No.8, Issue No.6, October – November 2020.
11. M. Vyshnavi, N. Abhigna, P. Laharika, "Fingerprint Authentication System for Vehicle Using GPS And GSM", Volume 12, Issue 11, Nov 2022.
12. C. S. Kiran, "Anti-theft Fingerprint Security System for Motorcycles Using Arduino UNO, GPS/GSM Module", Indian Journal of Science and Technology, Vol 12(42), DOI: 10.17485/ijst/2019/v12i42/145823, November 2019.
13. S. Amalia, R. Andari, J. Arif, "Comparison of Battery Electric Power Consumption in a Fingerprint System or a Motor Manual Lock System", Volume 10. No 1, January 2023.
14. Soukhya S M, Sonu G , L Karthik Narayan, "Fingerprint Recognition and its Advanced Features", International Journal of Engineering Research & Technology (IJERT), Vol. 9 Issue 04, April-2020.
15. R. B. Fernandez, D. T. R. Seroje, "Two-Way Motorcycle Authentication with Alerting and Tracking System Using Mobile Application", International Research Journal of Advanced Engineering and Science, Volume 7, Issue 3, pp. 246-255, 2022.
16. K. Purwanto, Iswanto, T. K. Hariadi, "Microcontroller- based RFID, GSM and GPS for Motorcycle Security System", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 3, 2019.