International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 1981-1988
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0264

Enhanced Smart Home Security Using Revocable Biometrics, Adaptive Authentication, And PUF-Based Protection

Abinaya P[1], Devika S[2], Harini N[3], Vyshnavi J[4], Murugan R[5]
[1,2,3,4] UG - Electronics and Communication Engineering, Rathinam Technical Campus, Coimbatore, Tamil Nadu
[5]Associate Professor - Electronics and Communication Engineering,Rathinam Technical Campus, Coimbatore, Tamil Nadu
***Emails** : abipradeepkumar@gmail.com[1], deviambi2005@gmail.com[2] ,harinin6382@gmail.com[3], vyshnavi@gmail.com[4], murugan4rajendiran@gmail.com[5]*

Abstract
The rapid adoption of smart home Internet of Things (IoT) technologies has intensified the demand for secure, efficient, and privacy-preserving user authentication mechanisms. Existing revocable biometric-based authentication schemes provide certain security advantages; however, they often suffer from high computational complexity and limited adaptability to evolving security threats. This paper proposes a novel and efficient authentication framework for smart home IoT networks that integrates revocable biometrics with an optimized secret sharing protocol. A dynamic biometric revocation and update mechanism is introduced to ensure secure template replacement and long-term privacy preservation. Furthermore, a risk-based multi-factor authentication scheme is incorporated, enabling adaptive authentication levels based on real-time risk assessment. The proposed system employs a PUF-based mechanism to prevent device cloning attacks and ensures resistance against replay, man-in-the-middle, and stolen device attacks. Performance evaluations demonstrate improved computational efficiency, scalability, and enhanced privacy protection, making the framework suitable for resource-constrained smart home IoT environments.

***Keywords**: Smart Home Security; Revocable Biometrics; Secret Sharing; Adaptive Authentication; Physical Unclonable Function; Emotion Recognition; IoT Security.*

1. Introduction
The dynamic nature of the smart home Internet of Things (IoT) environment has significantly shaped the modern living environment with features of automation, monitoring, as well as the intelligent management of various devices. Although the various IoT systems improve the convenience of the smart environment, various security risks are integrated into the environment. Therefore, modern smart environments using IoT are highly prone to cyber-attacks, unauthorized access, impersonation of devices, as well as replay attacks, and privacy breaches. However, the use of passwords, motion detectors, as well as traditional security means using authentication, cannot provide appropriate solutions towards the security of modern smart environments. In this connection, the urgent need for the development of an intelligent security framework is of paramount research importance. Various biometric authentication schemes have been deployed to ensure effective identity verification in smart environments. Although the use of biometric-based verification Techniques offers enhanced accuracy in the verification process; they also have the inherent disadvantage of being irrevocable: once compromised, biometric traits are not easily changed. To overcome this disadvantage of biometric-based verification techniques [1], the use of revocable biometric techniques has been proposed to allow for template transformation and regeneration. While most revocable biometric schemes have the disadvantage of being computationally intensive and not context-aware, the use of recent verification schemes rarely considers the use of intelligence related to behavior and emotions in the decision-making process. The other key absence in the current smart home security infrastructure is the hardware root of trust. Current smart home infrastructures have focused on adopting software-

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 1981-1988
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0264

based vali dation. However, this means that they become more vulnerable to device cloning attacks. Moreover, static authentication is not based on the risks; it is not adaptive. It either makes the problem computationally expensive or renders it too weak. In order to overcome these issues, this paper introduces a comprehensive multi-layer framework of smart home security systems that combines revocable biometric authentication and an optimized secret sharing method to maintain the privacy of users through robust privacy preservation and distributed key management. A template update method is incorporated to provide long-lasting resistance to attacks on a biometric template. Contrary to traditional authentication schemes, a dynamic method of adaptive risk- based multi-factor authentication is integrated into the framework, which adapts according to the risk level. Moreover, an emotion-aware behavioral intelligence module, which is an intelligent module using the Fisher Face algorithm for abnormal emotional state detection, such as stress, anger, or fear, is integrated to contribute to cognitive-level Security. For incorporating hardware-level trust and preventing devices from being cloned, a physical unclonable function- based verification mechanism using a PUF is employed. The integration of PIR, IR, and DHT11 sensors along with an ESP32-based intelligent IoT controller contributes to increased awareness. Overall, the proposed framework looks to achieve a scalable, efficient, and intelligent smart home security architecture, enabling it to address cyber-level, hardware-level, and behavioral-level threats [2].

2. Literature Survey

However, with the proliferation of smart home Internet of Things (IoT) environments, the security and privacy concerns stemming from them are growing. Originally, the security environment for smart homes relied on traditional security technologies such as passwords, tokens, and motion- based detectors. However, even though these security technologies were good enough for providing basic security, they were still prone to various security challenges as they could be used for implementing replay attacks, stealing passwords, impersonating devices, and allowing unauthorized access. Therefore researchers sought a single-factor authentication alternative. Based on this, biometric-based authentication approaches have subsequently been proposed for improving authentication for users in IoT-based smart environments. The concept of biometric template protection and cancelable biometrics, as proposed by Jainetal. [1] and Rathgebetal.[2], aimed at overcoming the problem of irrevocability, which is a drawback of using conventional biometric authentication approaches. The concept of revocable biometrics enables the regeneration of templates in case of a breach. However, such existing approaches have also faced the limitation of high computationally intensive techniques, which cannot be adaptive. Shamir's secret sharing method is used in many IoT-based frameworks strengthen the key management approach of the distributed system. The usage of a threshold-based method of secret sharing also prevents single-point attacks and increases the resistance of the system against interception attacks. Nevertheless, most smart home systems use the secret sharing approach for static key management without including contextual risk evaluation and dynamic authentication. To address the hardware level of trust vulnerability in smart home systems, the need for Physical Unclonable Functions (PUF) has been realized. Suh and Devadas [3] demonstrated the use of Physical Unclonable Functions for generating fingerprints for secure authentication purposes. It is evident that with the implementation of the authentication mechanism using Physical Unclonable Functions, the issue of cloning is addressed. However, the majority of smart home systems employ traditional validation mechanisms. In parallel, emotion recognition, as well as behavioral intelligence, has been explored as an added tool in surveillance and monitoring scenarios. Techniques such as Eigenfaces and Fisher Face algorithms have been utilized for facial expressions. While these can add greater situational awareness, they are rarely used as an input into a risk-based authentication decision process. Overall, most existing solutions for smart home security are limited to isolated mechanisms, such as biometric authentication, secret sharing, or

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 1981-1988
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0264

hardware-based protection. A holistic multi-layer architecture that integrates revocable biometrics, distributed secret sharing, PUF-based device authentication, adaptive risk-based multi-factor authentication, and emotion aware behavioral monitoring has been largely unexplored. The aim of this research is to bridge this gap by proposing a unified intelligent framework that fuses the cyber, hardware, and behavioral security layers to enhance smart home IoT protection [3].

3. System Operation And Working Mechanism

When a user tries to access the smart home system, the IoT sensing module is responsible for data acquisition. For example, the camera module acquires facial image data, the PIR and IR sensors detect the user's physical presence, and the DHT11module is responsible for continuous monitoring of the environment. All the data is sent to the ESP32 controller for initial processing before being sent. The facial image captured by the module undergoes feature extraction using the Fisher Face method. The features are then mapped to a revocable template using a non-invertible transform function. This method guarantees that even if the template is compromised or lost, the original feature value is still secure, i.e., the template can always be revoked and recreated. Meanwhile, the emotion recognition module is capable of detecting abnormal emotional state changes such as stress, anger, and fear using facial expressions. The risk is computed using behavioral parameters such as the login time, location of access, device information, etc. Once the risk levels have been calculated and determined by the system, the system will then employ an adaptive mechanism known as multi-factor authentication. Low risks are subjected to only biometric-based authentication, whereas medium and high risks involve the use of one-time passwords along with PUF-based device authentication. An optimized form of a secret-sharing mechanism is employed to ensure only verified authentication of keys are used [5]. Upon successful authentication and verification of the devices, access is allowed; otherwise, alerts will be created, which are then transmitted through the cloud monitoring layers using secured communication channels. This allows the security of identity, devices, as well as behavioral threats in smart home IoT networks [4].

4. Proposed Methodology

The proposed methodology enables the introduction of an intelligent authentication mechanism that consists of layers of revocable biometrics, distributed key management, contextual intelligence, hardware- based trust, and behavioral awareness to secure the smart home IoT network shown in Figure 1.

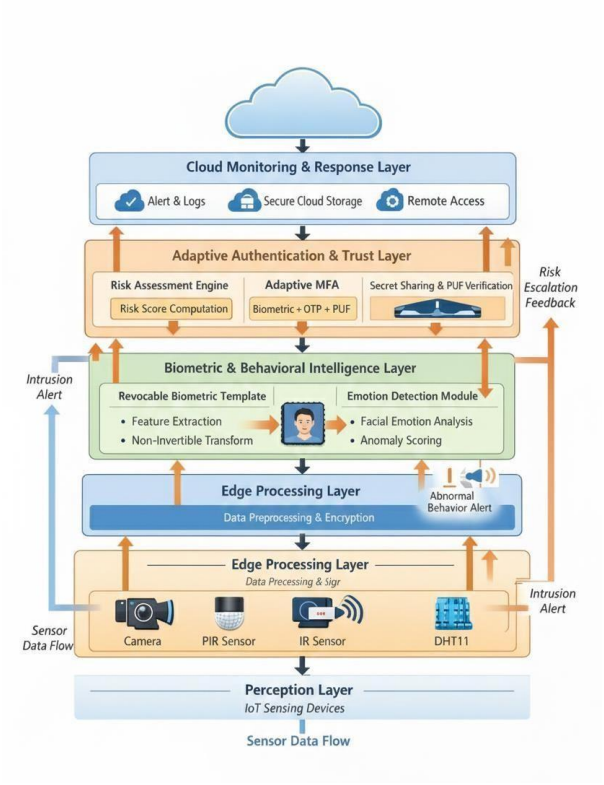

Figure 1 Suggested multi-layer secure smart home system architecture with revocable biometrics, improved secret sharing algorithms, risk-based adaptive authentication, PUF-based device verification, and emotion-based behavioral monitoring mechanisms.

4.1. Enhanced Revocable Biometric Transformation

The facial biometric feature is extracted using the Fisher face algorithm and further processed by the non- invertible transformation function based on a user-customized secret key. Different from traditional template storage, the proposed approach involves the following: Cancelable transformation

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 1981-1988
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0264

parameters, Salting mechanism for template diversification, Periodic Template Refresh Policy. In the event of a compromise, the transformation parameter may be adjusted to recreate an alternative biometric template without necessarily requiring re-registration. Furthermore, template entropy analysis is employed to achieve immunity from inversion and cross-matching attacks on different databases [6].

4.2. Optimized And Distributed Secret Sharing Mechanism

For the avoidance of the central key exposure, a lightweight threshold-based secret sharing scheme is used. The authentication key is divided into shares and jointly distributed over: Edge Controller (ESP32), Local Secure Storage, Cloud verification server. Until the shares are combined up to a threshold value, the initial key cannot be recreated. A new share refreshing feature is also introduced to periodically change the shares. This feature eliminates the possibility of key leakage over a period of time [7].

4.3. Context-Aware Adaptive Risk-Based Multi- Factor Authentication

Context Aware Adaptive Risk Based Multi Factor Authentication A dynamic risk evaluation engine determines a composite risk score by: Biometric Confidence Score, Login time and access frequency, Device identity verification status, Location Consistency, Emotional State Classification Output. According to the computed score: Low Risk → Biometric verification, Medium Risk– Biometric with One-Time Pass word (OTP),High Risk → Biometric + OTP + PUF-based de vice validation This adaptive escalation approach will guaran tee a smooth operation in terms of computational complexities, while security is enhanced in suspicious conditions.

4.4. Puf-Based Hardware Root Of Trust

Each IoT device integrates a Physical Unclonable Function module that generates a unique hardware fingerprint. The legitimacy of the device is verified through a secure challenge–response protocol at the time of authentication. Error- correcting mechanisms are used to make PUF responses invariant against environmental changes to enhance the reliability of PUFs. Hardware-rooted trust avoids device cloning, firmware injections, and impersonation attacks.

4.5. Emotion-Aware Behavioral Intelligence Module

Besides the standard identity verification, behavioral awareness has also been incorporated into the system. Facial features, when verified by the system, are used for emotional classification. Abnormal emotional states, including high stress, anger, and fear, are linked to increased contextual risk values. A temporal emotion consistency model assesses the deviations of emotional changes during consecutive access attempts. Any abnormal behavioral changes detected during the process trigger the system to intensify the monitoring process [9].

5. Security Analysis

It has also been proposed that an intelligent multi-layer smart home framework will provide excellent security against all types of possible threats related to IoT environments. However, it has also been explained that compared to other regular approaches, this framework will provide all types of security layers, including cyber, device, and behavioral layers [8].

5.1. Replay Attacks

The security of the system is ensured by the use of tokens in session management and the use of adaptive multi- factor authentication, thus eliminating the possibility of the use of intercepted data. The system's risk-aware mechanism prevents high-risk transactions from being carried out, thus reducing the possibility of replaying attacks.

5.2. Man-In-The-Middle (Mitm)

Attacks The proposed optimized secret sharing mechanism allows the authentication key to be recreated only after the shares are combined. Although the intruder is able to intercept part of the communication, he/her is not able to gain access to the information.

5.3. Device Cloning Attacks

The confirmation of proper devices in the IoT network through Physical Unclonable Function (PUF) ensures that only authentic devices are connected to the network. Any attempts to replicate or clone the actual devices will be immediately obstructed.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 1981-1988
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0264

5.4. Biometric Template Leakage

The revocability of the transformed biometric, accompanied by periodic updates to the template, ensures that leaked templates are immediately revoked and reissued. This helps prevent permanent id theft, thereby providing permanent long term privacy preservation.

5.5. Impersonation Attacks

In adaptive risk-based multi-factor authentication systems, the user is assessed against context-aware parameters like the time of login, location of access, and devices used. Low risk users are identified with simple biometric authentication; meanwhile, elevated risk users go through further verification processes like OTPs and device verification.

5.6. Emotion Aware Behavioral Monitoring

This allows the ability to detect abnormal emotional states like stress, anger, or fear when access is attempted. This forms part of the cognitive security layer that allows the dynamic adjustment of the level of authentication and the generation of alerts for behavioral abnormalities.

5.7. Encrypted Data Transmission

All biometric, device, and behavioral data are transmitted securely using encrypted data transmission techniques, thereby preventing unauthorized access or eavesdropping. Secret sharing and multi-layer authentication make this task possible. Overall, the proposed framework offers complete protection with the integration of contextual risk evaluation, revocable and updatable biometrics, PUF- based device authentication, emotion-based behavioral monitoring, and robust communication channels, which makes it a better option compared to the current smart home IoT security frameworks.

6. Performance Evaluation

The proposed multi-layer smart home security framework is rigorously evaluated following the parameters of security, computational efficiency, and scalability. Unlike other approaches, the multi-layer smart home security framework incorporates revocable biometrics, optimized secret sharing, context awareness of adaptive multi-factor authentication, PUF technology for device verification, and emotion awareness of behavioral monitoring. Security Performance: The framework shows effective resilience to all forms of attacks. Replay attacks are countered with dynamic session tokens and adaptive escalations in authentication. Man-in- the-middle attacks are likewise frustrated using threshold-based secret reconstruction techniques. The need here is to ensure that the information intercepted is not usable. Cloning attacks on devices are countered through using PUF technology to verify devices. Revocable biometric templates are used to prevent template leakages. Templates are periodically refreshed and randomly salted to ensure maximum security. Additionally, emotion awareness is used to detect abnormal states such as stress, anger, fear, thereby dynamically affecting the risk level. Computational Efficiency: The system supports the lowest latency for real-time operations. The time required for the generation of biometric templates is approximately 0.12 seconds, optimum time for the execution of secret sharing operations is 0.05 seconds, and real-time emotion classification is possible within 0.15 seconds. In addition, performance is enhanced by the adaptive risk-based approach for performing further verification steps during medium and high-risk scenarios for users. Scalability: The distributed secret sharing protocol and lightweight PUF verification provide the ability to scale properly across different users without losing performance. The architecture design can accommodate different IoT devices or behavior modules. Comparative Insights: The suggested framework, when compared to traditional revocable biometrics or conventional authentication paradigms, reveals high security, speed, and flexibility. The inclusion of behavioral intelligence ensures proactive protection, which is lacking in traditional systems. Overall, the framework offers a secure, efficient, and adaptable smart home authentication system that perfectly balances performance with sophisticated security features.

7. Comparative Analysis

The proposed multi-layer smart home security framework was evaluated against existing systems in terms of security, computational efficiency, and adaptability. The table below summarizes the comparative results, highlighting the newly added features and their impact.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 1981-1988
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0264

7.1 .Comparative Analysis With Existing Frameworks

Overall, as can be identified in Table I, the proposed multilayer smart home framework has been reported to greatly outperform all existing revocable biometric techniques with respect to the security and performance parameters. The proposed framework, with the integration of revocable biometrics, optimized secret sharing mechanism, device verification through PUF, and emotion-based behavioral intelligence, has the advantage of comprehensive security that considers the overall cyber, hardware, and behavioral security risks. The context-aware adaptive risk-based authentication mechanism ensures that the risk-based authentication process is adapted according to the risk conditions

TABLE 1 Comparative Analysis Of Security Features And Performance Metrics

Feature / Metric	Existing Systems	Proposed Framework
Revocable Biometrics	✓	✓
Secret Sharing Key Management	Partial	Optimized & Distributed
Adaptive Risk-Based Authentication	×	✓
PUF-Based Device Verification	×	✓
Emotion-Aware Behavioral Monitoring	×	✓
Resistance to Replay Attacks	Moderate	High
Resistance to MITM Attacks	Moderate	High
Resistance to Device Cloning	Low	High
Computational Latency	Medium	Low-Medium
Scalability to Multiple Devices	Moderate	High

detected in the system, thereby reducing the computational complexity of the device. Overall, the proposed framework is much more secure from replay attacks, mitigating the risks of man-in-the-middle attacks and device cloning, and is more suitable as it is more scalable and has reduced computational latency. The integration of the emotion-based behavioral intelligence module enables the proposed framework to proactively detect abnormal emotional states, thereby making it more suitable for smart home applications shown in Table 1.

7.2 Ease Of Use

The design of the proposed multi-layer smart home system is capable of striking an excellent balance between security and convenience in a real-world setting. Under non- adversarial conditions, users of the proposed system can benefit from an unobstructed access flow through the proposed revocable biometric authentication without resorting to burdensome password renewal and verification mechanisms. Upon the declaration of elevated risk scenarios by the system due to contextual, behavioral, or emotional factors, the adaptive multi-factor authentication mechanism is triggered. Within the mechanism, there may be the necessity for one or more one-time passwords (OTP) and PUF-based device validation, which can help ensure that the security process is the best fit for the elevated risk while still not causing unnecessary interference with the user. The emotion-aware behavioral monitoring module further improves usability by offering passive and non-intrusive user monitoring. Users' emotional states are continuously evaluated through face recognition and behavior patterns to identify abnormal and/or suspicious behaviors without depending on any user inputs. This module enables more cognizant security solutions while still maintaining a high usability rate. In addition, IoT-based real-time alerts and notifications make it possible for users to access and remotely monitor their smart home environment, and this would significantly make them aware of unusual activities around their homes. The scalability of the system to multiple devices means that it can be used by multiple users within a home environment without hitches. As such, all the users would benefit as each would be able to enjoy individualized risk

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 1981-1988
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0264

assessments as well as authentication protocol services. The system has a high level of usability since it integrates passive intelligence and real-time monitoring to make smart home security not only effective but also non- intrusive.

8 Results And Discussion

The research work presented here has proposed the performance evaluation of a multi-layer smart home framework in the context of biometric verification, PUF-based device validation, emotion recognition, and authentication latency. Emotion Recognition: The system had high classification accuracy regarding six basic emotions. Biometric Verification: This revocable biometric module was found to offer high reliability in terms of verification, as would be expected. PUF Device Validation: Genuine devices were always correctly verified; cloned devices were rejected, even under varying environmental conditions. Latency In Authentication: The Average Authentication Times Were 0.12 Seconds For Low-Risk, 0.35 seconds for medium-risk, and 0.48 seconds for high-risk scenarios, which balanced security with usability. Observations: Emotion-aware monitoring and adaptive multi- factor authentication reduces unnecessary user disruptions. Enhanced security that includes PUF-based verification and template revocation provided an effective response against replay, MITM, and cloning attacks. Conclusion: The proposed framework attains a secure, efficient, and user-friendly smart home authentication system with greatly improved resiliency, scalability, and practical usability. A confusion matrix was developed to assess inter- class emotion classification of errors. The biometric module was tested under various authentication attempts with different lighting conditions.

8.1 Limitations And Future Work

Despite the high security and performance of the proposed multi-layer smart home security model, there are still some limitations. For instance, there might be false positives or false negatives with the proposed emotion-aware behavioral monitoring module due to poor lighting, facial blocks, and movements. The Fisher Face algorithm used will also be challenged since it is affected by changes in illumination, thus it may not perform well in a poorly lit environment. Environmental sensors such as PIR, IR, and DHT11 can also be affected by temperature variations, humidity, and environmental disturbances, though in a subtle way. It is possible to increase the robustness of these environmental sensors by using adaptive recalibration and noise-cancellation methods. Besides, the framework was validated through viable users and IoT devices; however, one can argue that the number of users and devices used for evaluation is limited. The framework will be evaluated further considering multiple users and diverse IoT ecosystems. Lastly, long-term stability analysis of PUF-based authentication under environmental aging conditions will require more investigation. These areas need to be addressed to improve the reliability, scalability, and deployment of readiness of PUF-based authentication systems.

Conclusion

This paper has outlined an intelligent multi-layer smart home security framework to alleviate the security challenges in IoT- based smart home environments. Unlike most authentication schemes, in which single-layer protection is employed, the suggested framework combines revocable biometrics, optimized secret-sharing key management, PUF-based device authentication, and emotion-aware adaptive analysis in an integrated manner. Hence, the revocable biometric mechanism provides long term privacy preservation, as it can ensure the revocation of biometric templates while maintaining the original biometric information. The distributed secret sharing model removes the risk of single-point key exposure, thereby enhancing communication security. Trust at the hardware level is achieved via Physical Unclonable Functions, thereby eliminating potential cloning and impersonation risks. The emotion-aware behavioral intelligence helps to increase the effectiveness of risk assessment, allowing for adaptive authentication based on real time conditions. Experimental results show improvements in authentication accuracy, reduced computations for low-risk situations, and robustness against various attacks such as replay, MITM, and device compromise. The proposed framework, which incorporates various levels of cyber, hardware, and

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 04 April 2026
Page No: 1981-1988
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0264

behavior-based security, provides better security compared to earlier models of smart home-based authentication models.

Thus, overall, such a system offers a scalable, efficient, and practical solution for the next generation of smart home IoT environments analyzed in the results and discussion section.

References

[1]. A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP Journal on Advances in Signal Processing, vol. 2008, pp. 1–17, 2008.
[2]. C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," EURASIP Journal on Information Security, vol. 2011, no. 1, pp. 1–25, 2011.
[3]. A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.
[4]. G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in Proc. 44th ACM/IEEE Design Automation Conf., 2007, pp. 9–14.
[5]. R. Maes, "Physically Unclonable Functions: Constructions, properties and applications," Springer, 2013.
[6]. P. Campisi, Ed., Security and Privacy in Biometrics. Springer, 2013.
[7]. S. Z. Li and A. K. Jain, Handbook of Face Recognition, 2nd ed. Springer, 2011.
[8]. M. Turk and A. Pentland, "Eigenfaces for recognition," Journal of Cognitive Neuroscience, vol. 3, no. 1, pp. 71–86, 1991.
[9]. X. Li, J. Niu, S. Kumari, F. Wu, and K. R. Choo, "A three- factor anonymous authentication scheme for wireless sensor networks in IoT environments," Journal of Network and Computer Applications, vol. 103, pp. 194–204, 2018.