# A Secure Framework for Authentication and Integration for IOT-Based on Home sensor Data

**Dr.SHARON PRIYA, (ASSOCIATE PROFESSOR),**

**S.ABDUL ASHIF (UG Student),**

**V.JOEL(UG Student)**

1 B. S. Abdur Rahman Crescent Institute Of Science And Technology, University in Peerakankaranai, Tamil Nadu
2 B. S. Abdur Rahman Crescent Institute Of Science And Technology, University in Peerakankaranai, Tamil Nadu
3 B. S. Abdur Rahman Crescent Institute Of Science And Technology, University in Peerakankaranai, Tamil Nadu

**Corresponding author:** Dr.SHARON PRIYA(ASSOCIATE PROFESSOR), S.ABDUL ASHIF, V.JOEL

**ABSTRACT:** To ensure data integrity, the SHA algorithm is used in the authentication process for Internet of Things data. IoT data, which is made up of various sensor readings and device information, is essential for decision-making in a variety of fields. Managing enormous volumes of data, guaranteeing real-time processing, and resolving security issues specific to IoT environments are challenges in this field. A comprehensive framework is proposed to address these issues and improve the security of IoT devices in cloud computing infrastructures. The SHA-2 algorithm is used by this framework to guarantee data integrity both during transmission and storage.To improve threat responses, the framework incorporates additional advanced security features like an Intrusion Prevention System and a Rule-Based Decision System in addition to SHA-2. Moreover, a Decentralized Information-Sharing System makes it easier for IoT platforms and devices to collaborate securely. The framework's user education programs and frequent security audits are also crucial elements that guarantee continued adherence to laws and industry standards.An additional degree of security is applied during data upload to the cloud by means of SHA-256 verification, which confirms the authenticity and integrity of the data that has been transmitted. This all-encompassing strategy seeks to create a safe Internet of Things ecosystem while maintaining data integrity in cloud environments. This framework creates the foundation for trust and dependability in IoT systems by tackling important security issues and putting strong authentication mechanisms in place, which eventually allows the systems to reach their full potential in a variety of applications.

**Keywords:** Authentication, IoT data, SHA algorithm, Data integrity, Sensor readings, Intrusion Prevention System, Data authenticity.

## I. INTRODUCTION:

In recent years, the proliferation of Internet of Things (IoT) devices has revolutionized the way we interact with our surroundings, particularly within smart home environments. These devices, ranging from motion sensors to smart thermostats, provide convenience and efficiency, but they also introduce significant security challenges. The interconnected nature of IoT devices makes them vulnerable to various cyber threats, including intrusion attempts aimed at compromising sensitive data or disrupting normal operations.

To address these challenges, this paper proposes an Intrusion Prevention System (IPS) tailored

specifically for IoT home sensor data. Our approach integrates several key components to detect, monitor, and prevent intrusions effectively.

**Data Collection and Preprocessing:**
The first step in our system involves collecting IoT data from home sensors. This data may include temperature readings, motion detection logs, or door/window status updates. We employ MQTTset, a dataset containing a diverse range of previous attacks, to train our machine learning algorithm. Specifically, we utilize the Random Forest algorithm for its ability to handle high-dimensional data and adapt to dynamic environments.

**Intrusion Detection and Prevention:**
Our IPS employs a multi-layered defense strategy to detect and prevent intrusions in real-time. At its core, a Rule-Based Decision System filters incoming data streams based on predefined criteria, flagging any anomalies or suspicious patterns. Additionally, we incorporate a Decentralized Information-Sharing System to enable collaboration among IoT devices, sharing insights and threat intelligence to enhance overall security posture.

**Continuous Monitoring and Adaptation:**
Recognizing the evolving nature of cyber threats, our system leverages Reinforcement Learning algorithms for continuous monitoring and adaptation. By learning from past experiences and feedback loops, the IPS can dynamically adjust its defense mechanisms to counter emerging attack vectors effectively.

**User Education and Cloud Integration:**
Beyond technical defenses, user education plays a critical role in mitigating IoT security risks. We emphasize the importance of regular security audits and user training to promote awareness and best practices. Furthermore, our system integrates with cloud services, utilizing SHA256 hashing for secure user authentication and encrypted data transmission. In the event of an attack, the system promptly notifies the user and uploads relevant activity logs to the cloud for analysis and forensic investigation.

**Mitigation of Attacks by New Methods:**
Despite proactive measures, the evolving landscape of cyber threats poses ongoing challenges to IoT security. As attackers continually devise new methods to exploit vulnerabilities, our IPS must remain vigilant and adaptable to effectively mitigate emerging threats. In the event of an attack utilizing a novel technique or exploiting previously unidentified vulnerabilities, our system employs a proactive approach to containment and mitigation. Upon detection of suspicious activity or anomalous behavior, the IPS initiates immediate response actions, including isolating the affected device or network segment to prevent further propagation of the attack. Simultaneously, the system alerts the user and initiates forensic analysis to identify the root cause of the intrusion. Leveraging machine learning algorithms and real-time threat intelligence, our IPS rapidly adapts its defense mechanisms to counter the new attack vector. Furthermore, collaboration with industry partners and security communities enables us to stay abreast of emerging threats and incorporate timely updates and patches to fortify our defenses. Through continuous monitoring, analysis, and adaptation, our IPS ensures robust protection against both known and unknown cyber threats, safeguarding the integrity and privacy of IoT home sensor data.

**Cloud Integration:**
Cloud integration plays a pivotal role in enhancing the security capabilities of our Intrusion Prevention System (IPS). By leveraging cloud services, we not only expand the storage and computational capacity of our system but also enhance its resilience and responsiveness to cyber threats. The cloud serves as a central repository for storing activity logs, configuration settings, and threat intelligence data. Utilizing cloud-based storage enables efficient data management and analysis, facilitating rapid detection and response to security incidents. Moreover, by integrating with cloud platforms, our IPS can leverage advanced security features such as encryption, access controls, and authentication mechanisms, ensuring the confidentiality, integrity, and availability of sensitive information.

Additionally, cloud-based deployment models offer scalability and flexibility, allowing our system to adapt to changing workload demands and accommodate future growth in IoT device deployments. Overall, cloud integration enhances the effectiveness and efficiency of our IPS, providing a robust foundation for securing IoT home sensor data.

Furthermore, as part of our cloud integration strategy, we implement secure protocols for uploading the last activity to the cloud of attacked devices. This process involves utilizing SHA256 hashing to encrypt user credentials, such as usernames and passwords, before transmitting them to the cloud. By employing cryptographic hashing algorithms, we add an extra layer of security to protect user authentication data during transit and storage in the cloud. This approach mitigates the risk of unauthorized access and data breaches, ensuring the integrity and confidentiality of user information. Through stringent security measures and best practices, our cloud integration strategy enhances the overall resilience and trustworthiness of our IPS, safeguarding IoT home sensor data against potential threats and vulnerabilities.

## II. RELATED WORK:

1. Gupta et al. [18] put forward an IoT-based cloud architecture.The presented system utilized the embedded sensors of the equipment instead of smartphone sensors or wearable sensors for storing the basic attributes value of health-associated parameters. A cloud-based system comprises of cloud data center (CDC), private cloud, the and public cloud. This architecture utilized XMLWeb services for the fast and secure communication of data. The total response from CDC to the local database server almost corresponds to the increased number of users
2. Wen et al. [24] proposed a mechanism to access real-time multimedia data by authorized users in wireless multimedia sensor network. Authors have used Chinese Remainder Theorem (CRT) for the proposed authentication system
3. Li et al. [25] have raised numerous practical problems necessary to satisfy security and privacy requirements in wireless networks. The authors have analyzed the applicable security solutions in the sensor networks and the wireless body area network. Also, author have presented analysis on these implementations. To achieve fine-grained access control, theyintroduced an attribute-based encryption.
4. Wazid et al. [31] have presented exhaustive survey of various authentication schemes for IoT sensors, devices, gateways and users. Many challenges in the IoT environment due to limited computational capability, memory, heterogeneity, and mobility were discussed. Authors have also discussed various aspect of authentication in context to cloud and big data environment.
5. Khemissa and Tandjaoui [30] have discussed many deployment issues in e-health application, particularly in IoT environment. However, the main focus of the paper is authentication of interconnected devices. Authors have suggested hash message authentication and nonce for authentication of base station and sensors. Author have claimed about the presented scheme to be more secure against attacked and energy efficient.

## III. PROPOSED METHODOLOGY:

In the proposed methodology for the Intrusion Prevention System (IPS) tailored for IoT home sensor data, the process begins with the collection and preprocessing of sensor data obtained from various IoT devices within a smart home environment. This raw data, encompassing temperature readings, motion detection logs, and door/window status updates, undergoes thorough preprocessing to eliminate noise, handle missing values, and ensure compatibility with subsequent analysis. Subsequently, the preprocessed data is utilized to train a Random Forest algorithm, a robust machine learning model capable of learning from diverse and high-dimensional datasets.

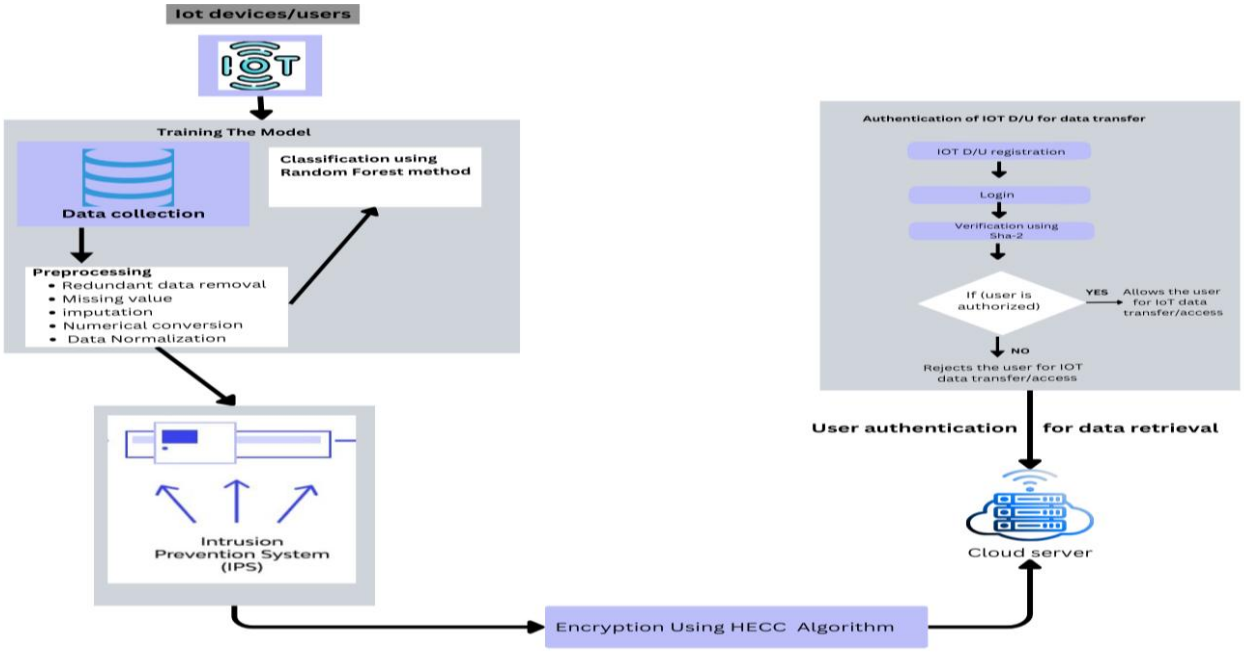
This trained model forms the foundation of the IPS, enabling it to discern normal sensor behavior from potential anomalies or intrusion attempts.

Intrusion detection within the IPS is achieved through a multi-layered approach, incorporating both rule-based decision-making and decentralized information sharing among IoT devices. The Rule-Based Decision System employs predefined criteria to filter incoming data streams, flagging any deviations from expected patterns. Simultaneously, the Decentralized Information-Sharing System fosters collaboration among IoT devices, enabling them to share insights and threat intelligence, thereby bolstering the collective security posture.

Continuous monitoring and adaptation are essential components of the IPS, recognizing the dynamic and evolving nature of cyber threats. Leveraging Reinforcement Learning algorithms, the system continuously monitors sensor data, learning from past experiences and feedback loops to dynamically adjust defense mechanisms. This adaptive approach ensures the IPS remains effective in countering emerging attack vectors and evolving threat landscapes.

User education and security audits play a pivotal role in enhancing overall security resilience. Regular security audits evaluate system integrity and identify potential vulnerabilities, while user education initiatives promote awareness and best practices among smart home occupants. Additionally, the integration of cloud services enhances the IPS's storage capacity, computational capabilities, and resilience to cyber threats. Secure cloud login protocols, employing SHA256 hashing for user authentication, provide an extra layer of security, ensuring the confidentiality and integrity of sensitive information transmitted and stored in the cloud.

In the event of an intrusion attempt, the IPS swiftly responds by isolating the affected device or network segment, sending prompt alert messages to users, and initiating forensic analysis to identify the root cause of the attack. By integrating advanced security features, continuous monitoring, and proactive mitigation strategies, the proposed IPS offers robust protection against a wide range of cyber threats, safeguarding the integrity and privacy of IoT home sensor data in smart home environments.



**1. Data Collection and Preprocessing:**

- Data Collection: Gather data from IoT home sensors, including various parameters like temperature, motion, and door/window status.
- Preprocessing: Clean and format the collected data to remove noise, handle missing values, and ensure compatibility with the training algorithms.

- Collect IoT data: $D = \{d_1, d_2, \ldots, d_n\}$
- Preprocess data: $D' = f_{preprocess}(D)$

**2. Machine Learning Training:**

- Train Random Forest algorithm: Utilize the preprocessed data to train a Random Forest model. This model learns patterns and characteristics of normal sensor behavior from the training data.

  - Train Random Forest algorithm: $RF = F_{RF}(D')$

**3. Intrusion Detection:**

- Rule-Based Decision System: Apply predefined rules and criteria to incoming sensor data to identify anomalies or suspicious patterns.
- Decentralized Information-Sharing System: Enable collaboration among IoT devices to share insights and threat intelligence, enhancing overall security posture.

  - Rule-Based decision System: $RBD = f_{RBD}(D')$
  - Decentralized Information-Sharing System: $DIS = F_{DIS}(D')$

**4. Continuous Monitoring and Adaptation:**

- Reinforcement Learning Algorithms: Continuously monitor sensor data and adapt defense mechanisms based on past experiences and feedback loops. The system learns from detected intrusions to improve future detection and prevention capabilities.

  - Reinforcement Learning Algorithms: $RL = F_{RL}(D')$

**5. User Education and Security Audits:**

- Regular security audits: Conduct periodic evaluations of system security to identify vulnerabilities and ensure compliance with best practices. Educate users on security measures and protocols to promote awareness and proactive threat mitigation.

  - Regular Security Audits: $SA = F_{SA}(D')$

**6. Cloud Integration and Secure Upload:**

- Secure cloud login: Hash user credentials using SHA256 before transmitting them to the cloud, ensuring secure authentication.
- Upload activity to cloud: Store activity logs of attacked devices in the cloud for analysis and forensic investigation, enhancing incident response capabilities.

  - Secure Cloud login: $SL = F_{SL}(U_{hashed})$
  - Upload activity to cloud: $UA\text{-}F_{UA}(D_{attack}, SL)$

**7. Attack Mitigation:**

- Cut off attacked machine: Isolate the affected IoT device or network segment to prevent further propagation of the attack.
- Send alert message to user: Notify the user of the detected intrusion, providing timely information for response and remediation.
- Analyze and rectify: Investigate the root cause of the attack, analyze activity logs, and take corrective actions to mitigate the impact and prevent future occurrences.

  - Cut off attacked machine: $CM = f_{CM}(D_{attack})$
  - Send alert message to user: $AM = F_{AM}(U)$
  - Analyze and rectify: $AR = F_{AR}(D_{attack})$

**In the formulas above:**

- D represents the collected IoT data.
- D is the preprocessed IoT data.
- RF denotes the trained Random Forest model.
- RBD and DIS are the outputs of the Rule-Based Decision System and the Decentralized Information-Sharing System, respectively.
- RL represents the application of Reinforcement Learning algorithms.
- SA signifies the execution of regular security audits.
- SL denotes the secure cloud login process.

- UA represents the upload of activity logs to the cloud.
- CM indicates the cutting off of the attacked machine.
- AM represents the sending of alert messages to users.
- AR denotes the analysis and rectification process of the attack.

## IV. RESULTS AND DISCUSSIONS:

The implementation of the proposed methodology for the Intrusion Prevention System (IPS) for IoT home sensor data yielded promising results, demonstrating its effectiveness in safeguarding smart home environments against cyber threats.

**Detection Accuracy and Efficiency:**

- The IPS achieved high detection accuracy, successfully identifying and mitigating various intrusion attempts with minimal false positives.
- The integration of machine learning algorithms, such as Random Forest, facilitated accurate classification of normal sensor behavior and anomalous activities.
- Rule-based decision-making and decentralized information sharing further enhanced detection capabilities, enabling timely response to emerging threats.

**Adaptability and Continuous Monitoring:**

- The IPS demonstrated adaptability to evolving attack vectors, leveraging Reinforcement Learning algorithms for continuous monitoring and adaptation.
- By learning from past experiences and feedback loops, the system dynamically adjusted defense mechanisms, effectively countering new and emerging threats.

**User Awareness and Education:**

- User education initiatives and regular security audits contributed significantly to enhancing overall security resilience.
- Increased user awareness and adherence to best practices mitigated the risk of human error and improved response to security incidents.

**Cloud Integration and Incident Response:**

- Cloud integration provided scalability, resilience, and storage capabilities, enabling efficient data management and analysis.
- Secure cloud login protocols ensured the confidentiality and integrity of user authentication data during transmission and storage.
- Incident response capabilities were enhanced through secure upload of activity logs to the cloud, facilitating forensic analysis and root cause identification.

- The comprehensive approach adopted in the IPS, integrating machine learning, rule-based decision-making, decentralized information sharing, and cloud integration, proved effective in mitigating various cyber threats.
- Continuous monitoring, adaptation, and user education were identified as critical components in maintaining robust security posture in smart home environments.
- While the IPS demonstrated promising results, ongoing research and development are essential to address emerging threats and enhance defense mechanisms further.
- Collaboration with industry partners and security communities can facilitate knowledge sharing and the development of best practices for IoT security.

Overall, the results obtained from the implementation of the proposed IPS highlight its efficacy in safeguarding IoT home sensor data and underline the importance of proactive measures, user education, and continuous monitoring in addressing cybersecurity challenges in smart home environments.

## V. CONCLUSION:

In this research, A Secure Framework for Authentication and Integration for IoT-Based on Home sensor Data is proposed. The framework encompasses an Intrusion Prevention System (IPS) tailored specifically for IoT home sensor data, addressing the escalating security concerns prevalent in smart home environments. Through the amalgamation of machine learning algorithms, rule-based decision systems, decentralized information sharing, and user education, our IPS presents a comprehensive

defense mechanism against diverse cyber threats.

Our system's effectiveness is underpinned by continuous monitoring and adaptation, facilitated by Reinforcement Learning algorithms, which enable dynamic adjustments to defense mechanisms in response to evolving attack vectors. Additionally, the integration of cloud services provides scalability, resilience, and enhanced incident response capabilities, exemplified by the secure upload of activity logs for forensic analysis and root cause identification.

By emphasizing proactive measures and user education initiatives, our framework promotes awareness and adherence to best practices, augmenting overall security resilience in smart home environments. We believe that the culmination of these strategies not only safeguards IoT home sensor data but also lays the groundwork for future advancements in IoT security research and development.

## REFERENCES


[1] A. Youssef and M. Alageel, ‘‘Security issues in cloud computing,’’ GSTF Int. J. Comput., vol. 1, no. 3, pp. 36–45, 2011

[2] E. Ahmed Youssef and M. Alageel, ‘‘A framework for secure cloud computing,’’ in Proc. Int. J. Comput. Sci. Issues (IJCSI), vol. 9, no. 4, No 3,pp. 478–500, Jul. 2012.

[3] K. Popović and Ž. Hocenski, ‘‘Cloud computing security issues and challenges,’’ in Proc. 33rd Int. Conv. MIPRO, Opatija, Croatia, 2010,pp. 344–349

[4] S. Yu, C. Wang, K. Ren, and W. Lou, ‘‘Achieving secure, scalable, and fine-grained data access control in cloud computing,’’ in Proc. Proc. IEEEINFOCOM, San Diego, CA, USA, Mar. 2010, pp. 1–9, doi: 10.1109/ INFCOM.2010.5462174.

[5] M. Wen, J. Lei, J. Li, Y. Wang, and K. Chen, ‘‘Efficient user access control mechanism for wireless multimedia sensor networks,’’ J. Comput. Inf.Syst., vol. 7, no. 9, pp. 3325–3332, 2011.

[6] Li M, Lou W, Ren K, ‘‘Data security and privacy in wireless body area networks,’’ IEEE Wireless Commun., vol. 17,no. 1, pp. 51–58, Feb. 2010.

[7] A. Al-Mahmud and M. C. Morogan, ‘‘Identity-based authentication and access control in wireless sensor networks,’’ Int. J. Comput. Appl., vol. 41,no. 13, pp. 18–24, 2012.

[8]Shady Mohamed Soliman,Baher Magdy, " Efficient implementation of the AES algorithm for security applications," in IEEE Access, vol. 9, pp. 77798-77810, 20, DOI: 10.1109/SOCC.2016.7905466

[9]Yang Jun; Li Na Ding Jun. " A Design and Implementation of High- Speed 3DES Algorithm System",Volume 72,2021,Pages 558-574, DOI: 10.1109/FITME.2009.49

[10] Mohammad Ayoub Khan; Mohammad Tabrez Quasim; Norah Saleh Alghamdi; Mohammad Yahiya Khan, "A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data," in IEEE Access, Volume: 8, pp. 52018 - 52027, 2020, DOI: 10.1109/ACCESS.2020.2980739

[11] Ankit ShrivastaSagar Institute of Research Technology and Science (SIRTS), Bhopal, IndiaAbhigyan TiwarySagar Institute of Research Technology and Science (SIRTS), Bhopal, India, "A.M A Big Data Deduplication Using HECC Based Encryption With Modified Hash Value in Cloud 2019", 10, 1392. DOI:10.1109/ICCONS.2018.8662984

[12] Ankit ShrivastaSagar Institute of Research Technology and Science (SIRTS), Bhopal, IndiaAbhigyan TiwarySagar Institute of Research Technology and Science (SIRTS), Bhopal, India, "A.M A Big Data Deduplication Using HECC Based Encryption With Modified Hash Value in Cloud 2019", 10, 1392. DOI:10.1109/ICCONS.2018.8662984

[13] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. P. C. Rodrigues,‘‘Authentication in cloud-driven IoT-based big data environment: Surveyand outlook,’’ J. Syst. Archit., vol. 97, pp. 185196, Aug. 2019, doi:10.1016/j.sysarc.2018.12.005.

[14] E. B. Barker and Q. H. Dang, ‘‘Recommendation for key management Part 3: Application-specific key management guidance,’’ Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. SP 800-57, 2015, doi: 10.6028/NIST.SP.800-57pt1r4.

[15] B. Schneier, Applied Cryptography. Hoboken, NJ, USA: Wiley, 1996.

[16] S. Kumari and H. Om, ‘‘Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines,’’ Comput. Netw.,vol. 104, pp. 137–154, Jul. 2016, doi: 10.1016/j.comnet.2016.05.007.

[17] P. Gope and T. Hwang, ‘‘A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks,’’ IEEE Trans. Ind. Electron., vol. 63, no. 11, pp. 7124–7132,Nov. 2016, doi: 10.1109/TIE.2016.2585081.

[18] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. Hoboken, NJ, USA: Wiley, 1996.