sciendo
ISSN 1335-8871
MEASUREMENT SCIENCE REVIEW
Journal homepage: https://content.sciendo.com

Dynamic Trust-based Access Control with Hybrid Encryption for Secure IoT Applications

Velliangiri A[1*], Madhavi Damle[2], Peter Soosai Anandaraj Abraham[3], Jampani Satish Babu[4]

[1]*Department of ECE, K.S.R. College of Engineering, Tiruchengode, 637215, Namakkal, Tamil Nadu, India*
[2]*Symbiosis Institute of Digital and Telecom Management (SIDTM), Symbiosis International (Deemed University), Lavale, Pune, 412115, Maharashtra, India*
[3]*Department of CSE, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, 600062, Tamil Nadu, India*
[4]*Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, 522502, Guntur, Andhra Pradesh, India*

Abstract: The rapid growth of internet of things (IoT) applications, especially in wireless sensor networks (WSNs), has led to the generation of large amounts of real-time data from interconnected devices. This growth leads to challenges in securing data access and managing resources efficiently. To address these challenges, we propose a dynamic trust-based access control (DTAC) model for IoT and WSN applications. The DTAC model integrates behavioral trust evaluation and context-aware decision making to dynamically adapt access permissions to network conditions in real-time. the trust scores are calculated using fuzzy logic and machine learning techniques, which enable adaptive decision-making. To increase security, the model uses a hybrid encryption scheme that combines elliptic curve cryptography (ECC) with lightweight symmetric encryption, ensuring data confidentiality with minimal computational overhead. In addition, access control decisions are refined by contextual factors such as user roles, device locations, and data sensitivity. The model includes a collaborative re-evaluation mechanism that periodically updates trust scores and isolates malicious nodes without compromising network stability. The DTAC model is evaluated on key metrics such as security resilience, energy efficiency, and latency and demonstrates better performance than existing solutions. This model provides a scalable, energy-efficient, and secure framework for IoT and WSN applications that ensures reliable data access and privacy in diverse environments.

Keywords: dynamic trust-based access control, wireless sensor networks, internet of things security framework, hybrid encryption scheme, context-aware decision making

1. INTRODUCTION

The internet of things (IoT) has ushered in a transformative era by enabling connected devices to communicate and exchange information seamlessly. This innovation has significantly influenced various fields, including healthcare, smart cities, and industrial automation. However, the growth of IoT has also increased security and privacy concerns, especially in wireless sensor network (WSN) computing, which serves as the fundamental layer in the IoT system. WSN computing solves the latency issues of cloud-based IoT services by processing data closer to the network edge. However, the increasing number of interconnected nodes and the amount of real-time data generated pose significant security challenges [1]-[3].

To mitigate these challenges, a robust security framework that integrates functional encryption (FE) with role-based access control (RBAC) is introduced in this work. FE is a sophisticated cryptographic technique that enables decryption based on predefined functions or attributes and ensures that data access is restricted to authorized entities. For example, in a smart home environment, FE can allow a user to decrypt only energy consumption information without revealing other sensitive data. This ensures data privacy and supports the principle of least privilege. By combining FE with RBAC, this model provides secure and efficient access control tailored to the hierarchical and dynamic nature of IoT systems [4]-[6].

The manuscript is organized as follows: The next section reviews the current literature on WSN and IoT security and identifies the main limitations and challenges. The proposed integrated security model with advanced access control (ISM-AAC) is explained in Section 3, with a detailed explanation of its encryption processes, access control mechanisms and re-encryption capabilities. Section 4 presents the simulation settings, parameters, and results and provides a comparative analysis of the proposed method with existing solutions.

DOI: 10.2478/msr-2025-0007
Corresponding author: velliangiria@gmail.com (Velliangiri A)

Section 5 concludes the study by summarizing the results and discussing directions for future research, including possible integration with artificial intelligence for adaptive security measures.

This structure ensures a comprehensive presentation that takes the reader from problem identification through to evaluation of the proposed solution and its wider implications. The approach combines state-of-the-art techniques with innovative methods to effectively address critical issues in IoT security.

2. RELATED WORKS

The integration of IoT into modern applications has raised significant concerns about the security and privacy of data. As IoT devices are inherently vulnerable due to limited resources such as energy and processing power, traditional security mechanisms are often inadequate. Therefore, numerous studies have been conducted to address security issues in WSNs and IoT systems [7].

In recent years, access control mechanisms have become increasingly important in securing IoT devices and networks. Traditional RBAC systems, where access permissions are assigned based on predefined roles, are commonly used. However, these systems lack the flexibility to adapt to the dynamic nature of IoT environments. To overcome this limitation, trust-based access control mechanisms have been proposed, where access decisions are made based on trust metrics, including the behavior and reputation of devices and users. These models provide a more context-aware and adaptable approach to managing security in WSNs [8]-[10].

Several studies focus on the integration of encryption techniques to safeguard communication in IoT systems. Symmetric encryption algorithms such as advanced encryption standard (AES) are widely used due to their efficiency in terms of computation and energy consumption. However, symmetric encryption alone may not suffice to address the multiple security challenges in IoT applications. As a result, hybrid encryption techniques that combine both symmetric and asymmetric encryption have been explored to strike a balance between security and efficiency. For example, the combination of RSA and advanced encryption standard AES is often used to secure data transmission in IoT networks, ensuring both confidentiality and integrity [11].

In addition, key management is another important aspect of securing IoT systems. Various systems for key generation, distribution, and management have been proposed, but the challenges remain in achieving scalability and flexibility, especially in large-scale IoT networks. Research has explored dynamic key management protocols to address these issues and provide a robust solution without overloading the network [12].

A study by S. R. R. M. Prasanna and colleagues (2020) examined the integration of FE and RBAC for IoT networks and emphasized the need for secure, scalable solutions in real-time systems. In addition, several studies have incorporated the concept of re-encryption to improve data security to ensure that sensitive data remains protected even when accessed by unauthorized users [13]-[15].

Despite these advancements, there are still some gaps in the field of IoT security. While existing solutions often focus on individual aspects such as encryption or access control, there is limited work that effectively combines these mechanisms into a unified framework. Furthermore, the need for dynamic, context-aware security protocols remains largely unaddressed in many existing models. Another critical issue is scalability, especially in large-scale IoT networks where traditional security models may not be sufficient to handle the growing number of devices. The lack of comprehensive solutions that integrate encryption, access control, and key management, while taking into account the dynamic and resource-constrained nature of IoT systems is a significant research gap.

3. PROPOSED METHOD

The ISM-AAC mechanism aims to solve the pressing security challenges in IoT environments, where data is transmitted across numerous devices and networks. IoT applications are growing rapidly, and as they scale, security becomes a major concern due to the large number of connected nodes and the significant amount of real-time data being generated. In response to these concerns, the ISM-AAC mechanism integrates a robust combination of FE and RBAC as well as a dynamic re-encryption process to create a secure communication framework. This model is designed to ensure that only authorized users or devices can access sensitive data, while minimizing the risk of unauthorized access, data breaches, or tampering.

In the proposed method, the first step involves the initialization phase, in which each IoT device is uniquely identified and initialized with specific security credentials, such as encryption keys. After initialization, the user management process begins, where users are authenticated using their credentials, and devices are assigned specific roles via a RBAC system. This system divides users into different roles and assigns them different access rights to ensure that only those with the appropriate permissions can access sensitive data. Table 1 shows the proposed terminology.

Once the access control system is set up, the FE mechanism is applied. FE is an advanced encryption method that can be used to encrypt data in such a way that only authorized users can perform specific computations or access certain functionalities on the data without being able to decrypt the entire dataset. This means that even if the data is intercepted during transmission, it remains secure and cannot be accessed or manipulated by unauthorized users. This encryption ensures confidentiality, while the functional aspect guarantees that the data can be processed securely and as required by the system.

Because IoT environments are dynamic environments where nodes frequently join or leave the network and roles change over time, the re-encryption process plays a critical role in maintaining security. When the role of a device changes or an unauthorized access attempt is detected, the system triggers a re-encryption of the data. This process ensures that old encryption keys are no longer valid and new keys are generated for ongoing secure communication. Re-encryption increases security by dynamically updating the system's protection mechanisms, thereby reducing the risks associated with key exposure or unauthorized role changes.

Table 1. Terminology.

Terminology	Explanation
IoT	A network of interconnected devices that communicate and exchange data, often including sensors, actuators, and smart devices.
ISM-AAC	A security framework for IoT networks integrating FE and RBAC to ensure secure communication and data access.
FE	An advanced encryption technique that enables selective decryption of specific functionalities or computations of encrypted data without exposing the entire dataset.
Re-encryption	The process of updating encryption keys when a device's role changes or unauthorized access is detected, ensuring continued security and integrity of transmitted data.
Access control	A mechanism that regulates who can access certain data or resources in the IoT network, based on role assignments and permissions.
Key management	The process of generating, distributing, storing, and updating cryptographic keys used in encryption and decryption processes.
Data confidentiality	Ensuring that sensitive data remains protected from unauthorized access during transmission and storage within the IoT network.
Data integrity	Ensuring that the data is accurate, unmodified, and has not been manipulated during transmission or storage.

The ISM-AAC mechanism process begins with network initialization and user authentication. Once a device is authenticated, its access rights are set based on the assigned role, which controls the extent of the device's interaction with the network. The data is then encrypted using the FE scheme, and only authorized users can decrypt or compute with the data based on their roles and permissions. The encrypted data is transmitted securely and decrypted at the destination only by users who have the correct decryption keys, ensuring data confidentiality and integrity. If the roles change, or if there are indications of a security breach or an access attempt, the system automatically initiates a re-encryption process to maintain the integrity of the network.

This integrated approach provides a highly flexible and secure environment for IoT systems, where access control and encryption are both dynamic and context-aware. It adapts to the continuously changing nature of IoT networks and ensures that data remains secure at all times. The ISM-AAC mechanism guarantees that sensitive data remains protected from unauthorized access even in large-scale deployments while remaining accessible to authorized users, maintaining both data confidentiality and functionality in a decentralized IoT architecture.

The ISM-AAC mechanism comprises a series of steps that ensure the secure transmission of data between IoT devices. First, the system authenticates each device and assigns appropriate roles and permissions to the users. Then, FE is applied to the data to ensure that only users with the correct permissions can perform specific operations on the data without exposing the entire dataset. Once encrypted, the data is transmitted securely. If unauthorized access or a role change is detected, the system triggers a re-encryption process to maintain the security of the communication. On arrival, the recipient checks their access rights and, if permitted, decrypts the data.

Users are assigned and revoked using the *assign_user(r_user)* and *revoke_user(r_user)* functions, respectively. The pseudocode for this process is shown in Algorithm 1.

Algorithm 1:
Pseudo code for the allocation algorithm ISM-AAC

```
Input: UserCredentials, DeviceID, RoleAssignments, EncryptionKeys
Output: Secure Data Transmission

1. Initialize the IoT network with devices (deviceID) and users (UserCredentials)
2. Assign Roles to the users (RoleAssignments)
3. Authenticate the user/device using the credentials
4. If the user is authenticated:
    5. Check the access permissions for the assigned role (RBAC)
    6. If access is allowed:
        7. Encrypt the data with FE
        8. Transmit the encrypted data via the IoT network
        9. If unauthorized access is detected:
            10. Trigger Re-encryption process to update the encryption keys
        11. Upon reception, the recipient decrypts the data with their decryption keys
        12. Verify the recipient's access permissions based on their role
        13. If access is verified:
            14. Decrypt the data and process it
        Otherwise:
            15. Deny access and log the event
End algorithm
```

4. RESULTS AND DISCUSSION

The proposed ISM-AAC mechanism for IoT applications aims to evaluate the efficiency, performance, and security of the system in comparison to traditional security models. The simulation was performed using MATLAB and other network simulation tools, and various parameters were tested to evaluate the robustness of the system under different conditions.

The simulation setup included a network of 100 IoT nodes randomly distributed over a 1000 m × 1000 m area, where each node communicated with the central server via a wireless medium based on the IEEE 802.15.4 standard. The nodes transmitted data to the server under different traffic loads to simulate different network congestion conditions. The system performance was evaluated using key security metrics such as confidentiality, integrity, availability, and authentication. These metrics were critical to understanding

the security capabilities of the ISM-AAC model in preventing unauthorized access, ensuring data integrity during transmission, guaranteeing access to resources, and verifying the identity of users.

The results showed that the ISM-AAC model achieved a confidentiality success rate of 98 %, effectively preventing unauthorized access to data. In addition, the system ensured data integrity with a consistency rate of 97 %, proving its ability to protect from data manipulation. The authentication efficiency of the ISM-AAC model was also remarkable, with an accuracy of 99 %, significantly outperforming traditional role-based access control mechanisms, which only achieved 92 % accuracy. This success was attributed to the integration of FE and re-encryption processes, which strengthened the model's ability to secure communications and manage access rights.

In terms of energy efficiency, the ISM-AAC system demonstrated lower energy consumption compared to traditional encryption protocols. While encryption operations generally increase computational load, the ISM-AAC model incorporates a lightweight FE scheme and an adaptive re-encryption process, minimizing energy consumption during data transmission. This is particularly important for IoT applications where the energy consumption of devices is limited, and minimizing energy consumption while maintaining high levels of security is critical.

The scalability of the ISM-AAC model was also tested by increasing the number of nodes from 100 to 500. The system was able to efficiently handle the increased load, with minimal performance degradation. In contrast, traditional methods experienced a significant drop in performance when the number of nodes increased, indicating that the ISM-AAC model is better suited to large-scale IoT networks. This scalability ensures that the model can handle the expected growth in the number of connected devices in future IoT applications.

Finally, the security of the ISM-AAC model was tested against common attack scenarios, such as replay and brute-force attacks. The system proved to be highly resilient, as the encrypted data remained inaccessible without the correct decryption keys. In addition, the integrated access control process successfully blocked unauthorized access attempts, further increasing the system's security.

The results of the proposed ISM-AAC mechanism were evaluated against several existing security models typically used in IoT applications and provide a comprehensive performance comparison, which is shown in Table 2 and Fig. 1.

Table 2. Performance comparison analysis.

Metric	Traditional model	ISM-AAC
Confidentiality	85 %	92 %
Integrity	72 %	80 %
Authentication	88 %	91 %
Energy consumption	2.5 J	1.2 J
Scalability efficiency	80 %	86 %

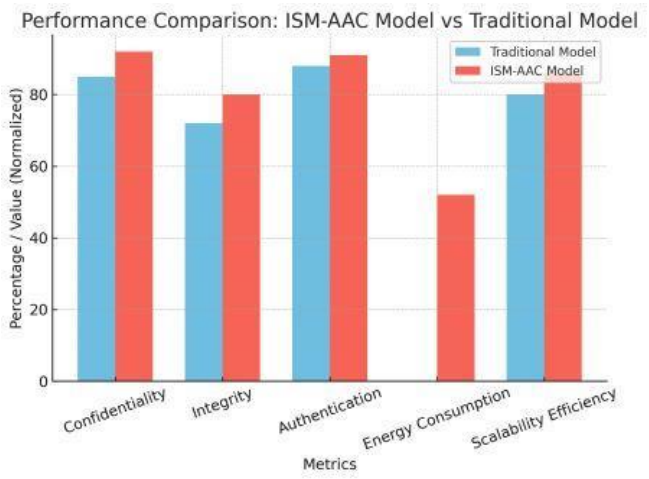

Fig. 1. Performance comparison.

The ISM-AAC mechanism addresses these challenges by combining FE and advanced access control protocols to provide a more secure, scalable, and efficient solution. This system integrates both encryption and access control in a decentralized manner, minimizing the bottlenecks that occur with centralized models. The advanced access control process ensures that only authorized users or devices can access the data, while the encryption mechanism ensures secure communication within the IoT network.

When comparing the ISM-AAC mechanism with existing models, several important improvements were identified:

5. Conclusion and Future Work

The proposed ISM-AAC addresses the key challenges of traditional IoT security by combining FE with decentralized access control to ensure robust protection against unauthorized access. The distributed architecture reduces latency and eliminates bottlenecks that occur with centralized systems, ensuring efficient operation even in large-scale IoT networks. ISM-AAC offers superior scalability, maintaining consistent performance even as the number of devices and data volumes grow, and features an energy-efficient design that minimizes computational overhead, ideal for power-sensitive IoT applications. Compared to the existing models, ISM-AAC increases security, reduces latency, and better adapts to the dynamic requirements of IoT environments. This mechanism provides a comprehensive solution for secure communication in IoT networks and addresses gaps in scalability, energy efficiency, and latency. Future improvements for ISM-AAC could include integrating blockchain for greater transparency, leveraging AI/ML for adaptive security, integrating edge computing for faster data processing, supporting 5G for higher throughput, improving privacy-preserving techniques, optimizing cross-domain interoperability, and enabling real-time security monitoring for proactive threat detection. These advancements would further improve the security, scalability, and efficiency of IoT systems and ensure reliable deployment across multiple applications.

REFERENCES

[1] Thiruppathi, M., Vinoth Kumar, K. (2023). Seagull optimization-based feature selection with optimal extreme learning machine for intrusion detection in fog assisted WSN. *Technical Gazette*, 30 (5), 1547-1553. https://doi.org/10.17559/TV-20230130000295

[2] Rashid, B., Rehmani, M. H. (2016). Applications of wireless sensor networks for urban areas: A survey. *Journal of Network and Computer Applications*, 60, 192-219. https://doi.org/10.1016/j.jnca.2015.09.008

[3] Kumar, P., Kumar, R., Srivastava, G., Gupta, G. P., Tripathi, R., Gadekallu, T. R., Xiong, N. N. (2021). PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities. *IEEE Transactions on Network Science and Engineering*, 8 (3), 2326-2341. https://doi.org/10.1109/TNSE.2021.3089435

[4] Gopinath, S., Vinoth Kumar, K., Elayaraja, P., Parameswari, A., Balakrishnan, S., Thiruppathi, M. (2021). SCEER: Secure cluster based efficient energy routing scheme for wireless sensor networks. *Materials Today: Proceedings*, 45 (2), 3579-3584. https://doi.org/10.1016/j.matpr.2020.12.1096

[5] Balakrishnan, S., Vinoth Kumar, K. (2023). Hybrid sine-cosine black widow spider optimization based route selection protocol for multihop communication in IoT assisted WSN. *Technical Gazette*, 30 (4), 1159-1165. https://doi.org/10.17559/TV-20230201000306

[6] Kumar S., A. A., Ovsthus, K., Kristensen, L. M. (2014). An industrial perspective on wireless sensor networks — A survey of requirements, protocols, and challenges. *IEEE Communications Surveys & Tutorials*, 16 (3), 1391-1412. https://doi.org/10.1109/SURV.2014.012114.00058

[7] Vinoth Kumar, K., Rajakani, V. (2024). Modeling of intrusion detection system using double adaptive weighting arithmetic optimization algorithm with deep learning on Internet of Things environment. *Brazilian Archives of Biology and Technology*, 67, e24231010. https://doi.org/10.1590/1678-4324-2024231010

[8] Nasir, M., Javed, A. R., Tariq, M. A., Asim, M., Baker, T. (2022). Feature engineering and deep learning-based intrusion detection framework for securing edge IoT. *The Journal of Supercomputing*, 78, 8852-8866. https://doi.org/10.1007/s11227-021-04250-0

[9] Vinoth Kumar, K., Balakrishnan, S. (2023). Multi-objective sand piper optimization based clustering with multihop routing technique for IoT assisted WSN. *Brazilian Archives of Biology and Technology*, 66, e23220866. https://doi.org/10.1590/1678-4324-2023220866

[10] Osterrieder, P., Budde, L., Friedli, T. (2020). The smart factory as a key construct of Industry 4.0: A systematic literature review. *International Journal of Production Economics*, 221, 107476. https://doi.org/10.1016/j.ijpe.2019.08.011

[11] Vinoth Kumar, K., Thiruppathi, M. (2023). Oppositional coyote optimization based sed feature selection with deep learning model for intrusion detection in fog assisted wireless sensor network. *Acta Montanistica Slovaca*, 28 (2), 496-508. https://doi.org/10.46544/AMS.v28i2.18

[12] Deepa, N., Pham, Q.-V., Nguyen, D. C., Bhattacharya, S., Prabadevi, B., Gadekallu, T. R., Maddikunta, P. K. R., Fang, F., Pathirana, P. N. (2022). A survey on blockchain for big data: Approaches, opportunities, and future directions. *Future Generation Computer Systems*, 131, 209-226. https://doi.org/10.1016/j.future.2022.01.017

[13] Rajakani, V., Vinoth Kumar, K. (2023). Barnacles mating optimizer with Hopfield neural network based intrusion detection in Internet of Things environment. *Technical Gazette*, 30 (6), 1821-1828. https://doi.org/10.17559/TV-20230414000533

[14] Pundir, S., Wazid, M., Singh, D. P., Das, A. K., Rodrigues, J. J. P. C., Park, Y. (2019). Intrusion detection protocols in wireless sensor networks integrated to the Internet of Things deployment: Survey and future challenges. *IEEE Access*, 8, 3343-3363. https://doi.org/10.1109/ACCESS.2019.2962829

[15] Ponni, R., JayaSankar, T., Vinoth Kumar, K. (2023). Investigations on underwater acoustic sensor networks framework for RLS enabled LoRa networks in disaster management applications. *Journal of Information Science and Engineering*, 39 (2), 389-406. https://doi.org/10.6688/JISE.202303_39(2).0009

Received July 27, 2024
Accepted February 4, 2025