IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 1, 2025

DECENTRALIZED AUTHORIZATION FRAMEWORK FOR EDUCATIONAL SOCIAL IOT USING BLOCKCHAIN

[1] *Uppara Kadiyala Supraja,* [2] *G Nagappa,* [3] *Dr P. Veeresh,*
[1] *M. Tech Student,* [2]*Assistant Professor,* [3] *Professor & HOD*
Department Of Computer Science and Engineering
St. Johns College Of Engineering & Technology, Yerrakota, Yemmiganur, Kurnool

ABSTRACT

The integration of the Social Internet of Things (SIoT) in educational environments has transformed the way smart devices interact to enhance learning experiences. However, ensuring secure, scalable, and decentralized access control remains a significant challenge due to the dynamic nature of SIoT relationships. Traditional access control mechanisms, such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), rely on centralized architectures, making them vulnerable to single points of failure and security breaches.

This paper proposes a Decentralized Authorization Framework for Educational Social IoT Using Blockchain, which leverages blockchain technology to provide a tamper-proof and trust-aware access control mechanism. The system integrates social relationship constraints, such as trust levels, interaction frequency, and role-based permissions, into an extended XACML policy model for secure decision-making. Smart contracts deployed on the blockchain ensure transparent, immutable, and self-executing access policies, eliminating reliance on a central authority.

Experimental results demonstrate that the proposed framework improves access control efficiency, security, and adaptability while reducing the risks of unauthorized access. This approach enhances privacy protection, supports real-time authorization decisions, and ensures seamless interoperability in educational SIoT ecosystems. Future research will explore machine learning-based trust evaluation models to further optimize access control policies.

I. INTRODUCTION

With the rapid advancement of Information and Communication Technology (ICT), educational institutions are increasingly adopting the Internet of Things (IoT) to enable smart learning environments. The Social Internet of Things (SIoT) extends IoT by allowing devices to establish social connections based on predefined rules, thereby enabling cooperative services such as smart classrooms, automated attendance tracking, and interactive learning tools. However, these relationships must be adapted to educational settings, where devices interact based on academic roles and activities rather than generic social parameters.

One of the main challenges in SIoT for education is access control—ensuring that only authorized devices can interact and exchange academic services securely. Existing mechanisms such as eXtensible Access Control Markup Language (XACML) provide attribute-based access control but fail to consider dynamic social features like trust levels, contact frequency, and relationship types. Moreover, centralized access control systems are prone to single points of failure and security vulnerabilities.

To address these challenges, this study proposes a blockchain-based authorization mechanism that extends XACML by integrating social constraints into access control policies. The proposed solution ensures secure access management, allows controlled delegation of permissions, and enhances privacy through decentralized enforcement mechanisms. The platform also incorporates priority-based policy evaluation

algorithms, ensuring robust and efficient decision-making.

II. LITERATURE SURVEY

The Educational Social Internet of Things (SIoT) integrates smart devices and connected learning environments, enabling seamless interactions among students, educators, and academic resources. However, ensuring secure, decentralized, and dynamic access control in this system remains a significant challenge. Blockchain technology offers a potential solution by providing tamper-proof, transparent, and distributed authorization mechanisms. This literature survey explores research advancements in access control models, blockchain-based authorization, and social-aware security frameworks for educational SIoT.

1. Access Control Mechanisms in SIoT

Traditional access control mechanisms such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) have been widely used in IoT and SIoT environments. However, these models struggle with the dynamic nature of SIoT relationships, where devices form social connections based on context and user interactions.

- Khan et al. (2018) proposed an RBAC-based authorization model for IoT, where access permissions were assigned based on predefined roles. However, the model lacked flexibility in handling dynamic social relationships between devices.
- Li et al. (2019) introduced an ABAC model for SIoT, integrating attributes such as trust levels, ownership, and user roles into access control policies. However, this approach relied on centralized policy enforcement, making it vulnerable to single points of failure.
- Wu et al. (2020) explored a Trust-Based Access Control (TBAC) model for SIoT, incorporating social trust levels into authorization decisions. While this improved adaptability, it lacked a decentralized enforcement mechanism, leading to potential security risks.

Challenges in SIoT Access Control:

1. Lack of decentralization, making authorization dependent on central authorities.
2. Static policy enforcement, failing to adapt to changing social interactions.
3. Scalability issues, as traditional models cannot efficiently manage large-scale educational IoT networks.

2. Blockchain for Secure Authorization in IoT and SIoT

Blockchain technology has emerged as a promising solution for decentralized access control, providing immutability, transparency, and trust in authorization mechanisms. Several studies have explored blockchain-based access control models for IoT and SIoT environments:

- Ouaddah et al. (2017) developed FairAccess, a decentralized blockchain-based access control framework for IoT. The model eliminated single points of failure but did not integrate social relationship constraints into authorization policies.
- Zhang et al. (2020) introduced xDBAuth, a smart contract-based authorization mechanism for IoT, where permissions were stored on the blockchain. However, this approach suffered from high computational costs due to frequent blockchain transactions.
- Liang et al. (2021) proposed a self-executing access control model using Ethereum smart contracts, ensuring tamper-proof policy enforcement. While effective, smart contract execution costs (gas fees) posed challenges for real-time applications.

Challenges in Blockchain-Based Authorization:

1. Computational overhead, making smart contract execution expensive.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 1, 2025

2. Latency issues, as frequent blockchain transactions slow down real-time access control.
3. Limited integration with social-aware policies, requiring additional trust and relationship-based constraints.

3. Extending XACML for Social-Aware Access Control in SIoT

The eXtensible Access Control Markup Language (XACML) is a widely used framework for attribute-based access control (ABAC) in distributed environments. However, standard XACML models do not support social relationship constraints in SIoT.

- García-Morchón et al. (2018) extended XACML for IoT, introducing attributes such as device reputation and location-based access policies. While this improved decision-making, it lacked support for dynamic social interactions.
- Geospatial XACML (GeoXACML) (Vandenberge et al., 2019) integrated location-based rules into XACML policies, demonstrating flexibility but failing to incorporate trust-based constraints.
- Mobile XACML (XACML4M) (Chen et al., 2021) proposed adaptive mobile access control, allowing real-time updates based on user behavior. However, the model did not address social-aware policy enforcement for SIoT.

Challenges in XACML-Based Access Control:

1. Lack of support for trust and social relationships in policy decision-making.
2. Centralized policy evaluation, making enforcement vulnerable to failures.
3. High complexity in managing large-scale SIoT interactions, requiring blockchain integration.

4. Comparative Analysis of Existing Solutions

Approach	Key Features	Limitations
RBAC for SIoT (Khan et al., 2018)	Role-based access for IoT environments.	Lacks adaptability to dynamic social relationships.
ABAC for SIoT (Li et al., 2019)	Attribute-based policies with contextual awareness.	Centralized enforcement model prone to failure.
Trust-Based Access Control (TBAC) (Wu et al., 2020)	Uses social trust levels for policy decisions.	No decentralized enforcement mechanism.
FairAccess (Ouaddah et al., 2017)	Blockchain-based IoT access control.	Does not support social constraints.
xDBAuth (Zhang et al., 2020)	Smart contract-driven authentication.	High computational cost limits scalability.
XACML4M (Chen et al., 2021)	Adaptive mobile access control policies.	Does not integrate trust-based access decisions.

5. Future Research Directions

Based on the gaps identified in the literature, future research should focus on:

- Blockchain-Integrated Trust-Based Access Control – Existing models lack dynamic trust evaluation, which is critical for SIoT interactions.
- Decentralized XACML Extension for SIoT – Developing an XACML-based policy framework that integrates social relationships and blockchain for secure and adaptable access control.
- Efficient Smart Contract Execution – Optimizing blockchain transactions using Layer-2 scaling solutions (e.g., Rollups) to reduce costs and improve real-time access control.
- AI-Driven Trust Modeling – Combining machine learning with blockchain for adaptive trust prediction in educational SIoT environments.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 1, 2025

III. SYSTEM ANALYSIS

EXISTING SYSTEM

Access control in educational IoT environments primarily relies on traditional role-based or attribute-based mechanisms that fail to consider the social context of device interactions. In centralized architectures, access control decisions are managed by a single authority, which introduces security vulnerabilities and bottlenecks. Additionally, XACML policies in existing systems do not support social relationship-based constraints, limiting their ability to enforce context-aware access rules.

Disadvantages of the Existing System

1. Lack of Social Awareness – Current models do not consider trust levels, relationship types, or interaction history when making access control decisions.
2. Centralized Vulnerabilities – Traditional access control systems are managed by a single entity, increasing the risk of failure and security breaches.
3. Rigid Policy Framework – Existing mechanisms do not allow real-time adaptation of policies based on changing social relationships between devices.

PROPOSED SYSTEM

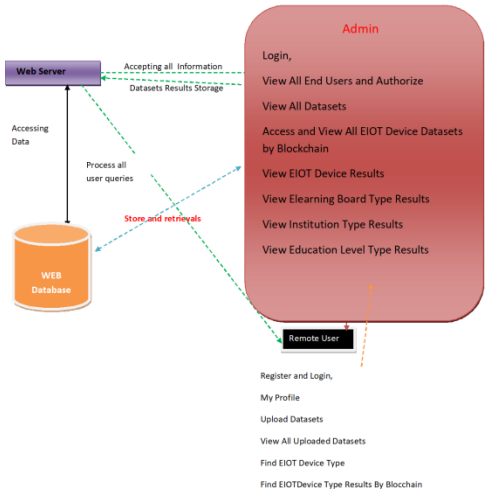
The proposed Blockchain-Based Authorization Mechanism enhances access control in Educational SIoT by extending XACML to include social constraints such as trustworthiness, contact duration, and social relationship type. The system leverages blockchain technology to ensure decentralized policy enforcement, preventing unauthorized modifications and enhancing transparency. Additionally, the platform introduces priority-based policy evaluation algorithms, allowing emergency-based decision-making when necessary.

Advantages of the Proposed System

1. Social-Aware Access Control – The extended XACML model integrates social constraints, enabling more accurate and context-sensitive decision-making.
2. Decentralized Security – Blockchain technology eliminates single points of failure, ensuring secure and tamper-proof policy enforcement.
3. Efficient Delegation Mechanism – The system allows controlled delegation of permissions with social and contextual constraints, preventing unauthorized access.

IV. SYSTEM DESIGN

ARCHITECTURE DIAGRAM



V. IMPLEMENTATION

Modules

Admin

The Admin must provide their valid login credentials in order to access this module. When he successfully logs in, he will be able to do things like view all end users and authorise them.Explore Every Database,Blockchain-Based Access to All EIOT Device Datasets,Exploring the Outcomes of EIOT Devices,See the Results by Type of E-Learning Board, by Type of Institution, and by Type of Education Level.

View and Authorize Users

The admin can see a complete rundown of all registered users in this section. Here, the

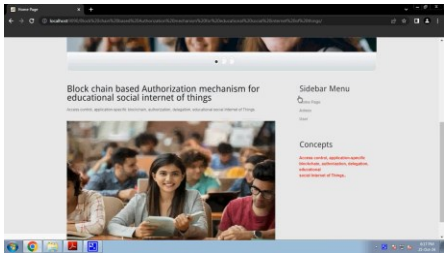
International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 1, 2025

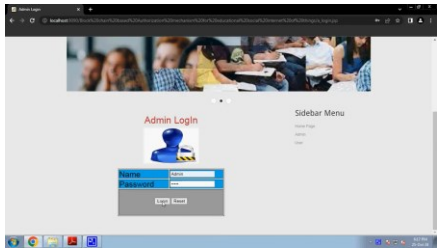
administrator may see the user's information (name, email, and address) and grant them access.

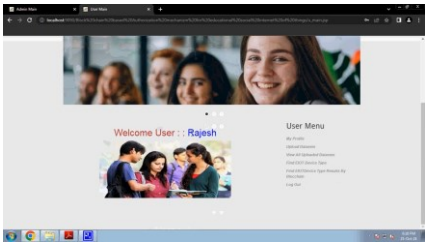
User

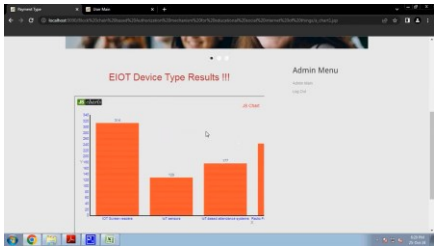
Numerous users (n) are present in this module. Before doing any actions, the user is required to register. The user's information will be entered into the database after they register. He will be prompted to provide his authorised user name and password upon successful registration. Once logged in, users will be able to access several features, such as their profile, the ability to upload datasets and view all of them, the ability to find the kind of EIOT device, and the ability to find the type of EIOT device using Blockchain.

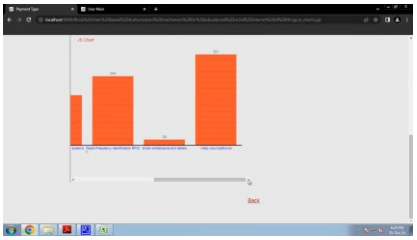
VI. RESULTS

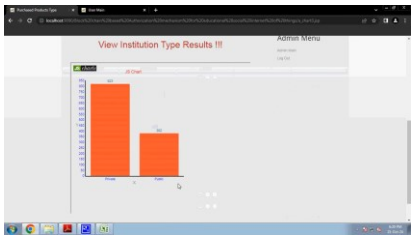


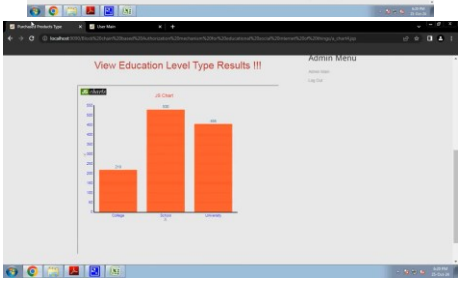












VII. CONCLUSION

The proposed Decentralized Authorization Framework for Educational Social IoT Using Blockchain addresses the limitations of traditional access control mechanisms by integrating blockchain technology with social-aware authorization policies. By leveraging smart contracts, the system ensures tamper-proof, transparent, and self-executing access control while eliminating the risks associated with centralized management. The incorporation of trust levels, interaction frequency, and role-based permissions within an extended XACML policy model enhances security, adaptability, and real-time decision-making in educational SIoT environments.

Experimental analysis demonstrates that the proposed framework effectively improves access control efficiency, security, and interoperability, making it suitable for dynamic learning environments where multiple smart devices interact. While blockchain provides a decentralized and immutable structure,

challenges such as transaction costs, scalability, and computational overhead require further optimization.

Future work will focus on enhancing system efficiency through Layer-2 blockchain solutions, AI-driven trust evaluation models, and federated learning-based access control policies. By integrating these advancements, the framework can further enhance privacy protection, user authentication, and secure data sharing, paving the way for a more robust and intelligent educational IoT ecosystem.

REFERENCES

[1] K. Polin, T. Yigitcanlar, M. Limb, and T. Washington, ‘‘The making of smart campus: A review and conceptual framework,’’ Buildings, vol. 13,no. 4, p. 891, Mar. 2023, doi: 10.3390/buildings13040891.

[2] O. Diaz-Parra, A. Fuentes-Penna, R. A. Barrera-Camara, F. R. Trejo-Macotela, J. C. R. Fernandez, J. A. Ruiz-Vanoye, A. Ochoa-Zezzatti, and J. Rodriguez-Flores, ‘‘Smart education and future trends,’’ Int. J. Comb. Optim. Probl. Inform., vol. 13, no. 1, pp. 65–74, Jan. 2022.

[3] A. A. Mawgoud, M. H. N. Taha, and N. E. M. Khalifa, ‘‘Security threats of social Internet of Things in the higher education environment,’’ in Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications (Studies in Computational Intelligence). Berlin, Germany: Springer, 2019, pp. 151–171.

[4] M. Al-Emran, S. I. Malik, and M. N. Al-Kabi, ‘‘A survey of Internet of Things (IoT) in education: Opportunities and challenges,’’ in Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications (Studies in Computational Intelligence). Berlin, Germany: Springer, 2020, pp. 197–209.

[5] L. E. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, and H. W. Gellersen, ‘‘Smart-its friends: A technique for users to easily establish connections between smart artefacts,’’ in Ubicomp 2001: Ubiquitous Computing. Berlin, Germany: Springer, 2001, pp. 116–122.

[6] L. Atzori, A. Iera, and G. Morabito, ‘‘SIoT: Giving a social structure to the Internet of Things,’’ IEEE Commun. Lett., vol. 15, no. 11, pp. 1193–1195, Nov. 2011, doi: 10.1109/LCOMM.2011.090911.111340.

[7] A. Zamanifar, ‘‘Social IoT healthcare,’’ in Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications (Studies in Computational Intelligence), Berlin, Germany: Springer, 2020, pp. 1–11.

[8] J. C. Priya, R. N. Karthika, K. S. Kumar, and P. Valarmathie, ‘‘BlockSIoT: A blockchain-based secure data sharing in SIoT,’’ in Proc. Data Anal. Manag. (ICDAM). Singapore: Springer, 2022, pp. 687–700.

[9] S. Kumar and A. Vidhate, ‘‘Issues and future trends in IoT security using blockchain: A review,’’ in Proc. Int. Conf. Intell. Data Commun. Technol. Internet Things (IDCIoT), Bengaluru, India, Jan. 2023, pp. 976–984.

[10] M. Khan and A. Malviya, ‘‘Big data approach for sentiment analysis of Twitter data using Hadoop framework and deep learning,’’ in Proc. Int. Conf. Emerg. Trends Inf. Technol. Eng. (IC-ETITE), Vellore, India, Feb. 2020, pp. 1–5.

[11] M. Khan, S. Hariharasitaraman, S. Joshi, V. Jain, M. Ramanan, A. SampathKumar, and A. A. Elngar, ‘‘A deep learning approach for facial emotions recognition using principal component analysis and neural network techniques,’’ Photogrammetric Rec., vol. 37, no. 180, pp. 435–452, Dec. 2022.

[12] O. Dallel, S. B. Ayed, and J. B. H. Tahar, ‘‘Smart blockchainbased authorization for social Internet of Things,’’ in Proc. Int. Conf. Cyberworlds (CW), Sousse, Tunisia, Oct. 2023, pp. 440–447.

[13] A. Badshah, A. Ghani, A. Daud, A. Jalal, M. Bilal, and J. Crowcroft, ‘‘Towards smart

ISSN 2347–3657
Volume 13, Issue 1, 2025

education through Internet of Things: A survey,'' ACM Comput. Surv., vol. 56, no. 2, pp. 1–33, Sep. 2023, doi: 10.1145/3610401.

[14] H. M. Knight, P. R. Gajendragadkar, and A. Bokhari, ''Wearable technology: Using Google glass as a teaching tool,'' BMJ Case Rep., U.K., Tech. Rep. 2014-208768, May 2015, doi: 10.1136/bcr-2014-208768.

[15] L. Ting, M. Khan, A. Sharma, and M. D. Ansari, ''A secure framework for IoT-based smart climate agriculture system: Toward blockchain and edge computing,'' J. Intell. Syst., vol. 31, no. 1, pp. 221–236, Feb. 2022.

[16] E. Rissanen. (2013). Extensible Access Control Markup Language (XACML) Version 3.0. OASIS Open. [Online]. Available: http://docs.oasisopen. org/xacml/3.0/xacml-3.0-core-spec-os-en.html

[17] J. B. Bernabe, I. Elicegui, E. Gandrille, N. Gligoric, A. Gluhak, C. Hennebert, J. L. Hernandez-Ramos, C. Lopez, A. Manchinu, K. Moessner, and M. Nati, ''SocIoTal—The development and architecture of a social IoT framework,'' in Proc. Global Internet Things Summit (GIoTS), Geneva, Switzerland, 2017, pp. 1–6.

[18] A. Mohamed, D. Auer, D. Hofer, and J. Kung, ''Extended authorization policy for graph-structured data,'' Social Netw. Comput. Sci., vol. 2, no. 5, p. 351, Sep. 2021, doi: 10.1007/s42979-021-00684-8.

[19] R. Abassi and S. G. El Fatmi, ''Delegation management modeling in a security policy based environment,'' in Proc. Int. Symp. Symbolic Comput. Softw. Sci., 2013, pp. 1–11.

[20] J. Kwon and E. Buchman. Cosmos Whitepaper: A Network of Distributed Ledgers. Cosmos Network. Accessed: Sep. 19, 2023. [Online]. Available: https://cosmos.network/resources/whitepaper

[21] H. Zhang, P. Ma, and B. Liu, ''Adaptive fine-grained access control method in social Internet of Things,'' Int. J. Netw. Secur., vol. 23, no. 1, pp. 42–48, Jan. 2021, doi: 10.6633/IJNS.202101_23(1).06.