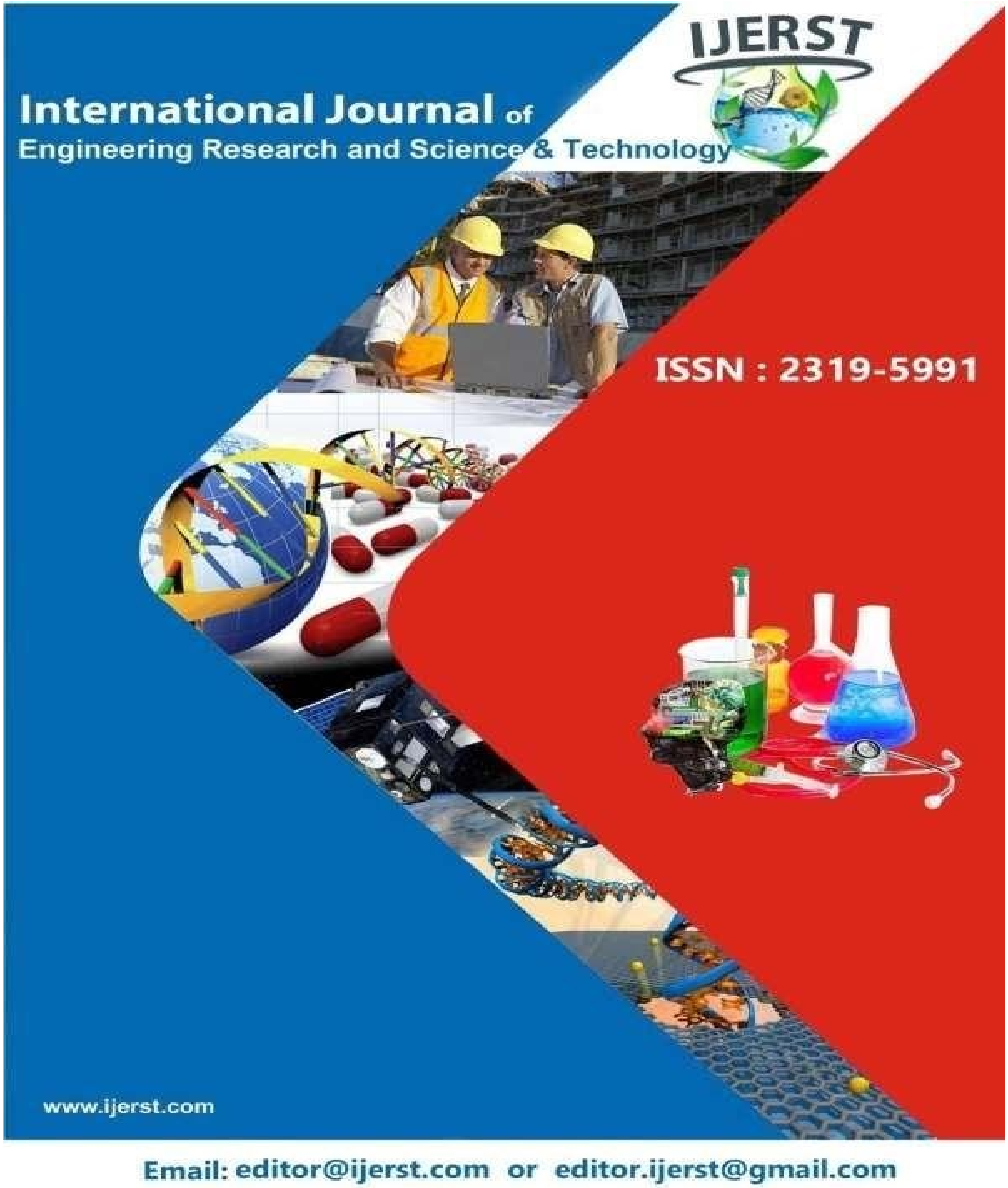


Email: editor@ijerst.com or editor.ijerst@gmail.com

Int. J. Eng. Res. & Sci. & Tech. 2025

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp1074-1082 Vol. 21, Issue 2, 2025

ENHANCING ACCESS CONTROL IN EDUCATIONAL SIOT USING BLOCKCHAIN TECHNOLOGY

[1]M. Hemalatha, MCA Student, Department of MCA

[2] Dr.M.Veeresha, Ph.D, Professor, Department of MCA

[12]Dr KV Subba Reddy Institute of Technology, Dupadu, Kurnool

ABSTRACT

In order to allow educational IoT devices to form social connections and provide academic services, the Social Internet of Things (SIoT) paradigm has been incorporated into the education sector. In the educational setting, however, where gadgets must be socially connected according to their academic responsibilities and activities, the social links are not adjusted. Additionally, the implementation of an access control mechanism becomes increasingly necessary as a result of the interchange of services. Social limitations, such the kind of social interaction and the frequency of communication, are important considerations when making an access choice in the Internet of Things. Nevertheless, these limitations cannot be defined as contextual conditions or device characteristics using the eXtensible Access Control Markup Language (XACML) standard. In this work, we propose an application-specific blockchain-based Educational Social Internet of Things (EducationalSIoT) platform where we define new social interactions for educational gadgets. We propose expanding the XACML policy model to take social considerations into account in order to limit access to academic services. In light of this, we modify the policy assessment procedure and provide priority-based combining algorithms. Furthermore, by establishing delegation norms and managing the delegation process while taking social aspects into account, our platform guarantees the transfer of access rights. According to the simulation findings, a delegation request is reviewed in 0.32 ms and an access request in 0.22 ms when social elements are included. Lastly, we promise that our platform is safe against replay and man-in-the-middle assaults.

I. INTRODUCTION

Without technology, education loses all of its value. Many educational institutions, including colleges and schools, are investing in implementing Internet of Things (IoT) technology due to the recent advancements in ICT and its influence on changing domains [1]. In order to provide smart services like smart pedagogy, smart classrooms, and smart administration, the Internet of Things is transforming conventional education into smart education [2]. An emerging paradigm known as the Social Internet of Things (SIoT) [6] is the result of combining the IoT with the social network notion [5] to expand its potential with cooperative services like service discovery. Social networking concepts are applied to the Internet of Things via SIoT [7]. By establishing social relationships on their own while adhering to the socialisation guidelines established by their owners, it enables smart gadgets to become social. The SIoT has been merged with blockchain technology, also known as Distributed Applications (DApps), to address the scalability of IoT devices and provide a decentralised architecture (e.g. BlockSIoT [8]). However, the limitations of DApps blockchain technology, the inability of social relationships to adapt to the educational context, and the need

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp1074-1082
Vol. 21, Issue 2, 2025

for secure access to academic services are three major obstacles to the applicability of blockchains combined with the SIoT in the educational context.

DApps like Ethereum, on the one hand, are often used for their distributed design, lack of a central authority, transaction recording, and transparency [9]. Only by using smart contracts can the business logic of DApps be altered. However, because of the solidity language's nascent environment, smart contracts pose obstacles to the creation of more sophisticated applications. For example, they are unable to use deep learning or machine learning models [10], [11] to create smart blockchains [12], which use data to train models and make intelligent judgements. They also need to be re-deployed with any updates. However, the Internet of Educational Things (IoET) is a new subcategory of IoT that includes wearable and portable gadgets (like smart glasses) and IoT devices used in educational settings (like smart whiteboards) [13]. For broad SIoT objectives, social linkages like co-location and co-work relationships [6] are used. For example, during class, the teachers let their tablets create social connections with the smart whiteboard for collaborative work. The social connections made between IoET devices must be tailored for the educational setting, however. For instance, the teacher may use his laptop to stream a video to medical students' and trainees' smart glasses to describe a medical operation [14]. Only pupils using the same class's smart glasses must be able to connect socially with the instructor's laptop. Therefore, we must identify new kinds of social connections that may be formed between IoET devices based on their academic responsibilities and activities, in addition to the social relationships suggested for SIoT.

Furthermore, the need to regulate access to these resources (i.e., data and services) is increased by the flow of data and services across social devices [15]. The eXtensible Access Control Markup Language (XACML) [16] is used to construct an authorisation component, as the SocIoTal example [17], in order to offer an effective protection and prevent unauthorised access. The OASIS standards group defined XACML, a fine-grained, attribute-based authorisation policy definition language [18]. It suggests a policy model in which a policy comprises a collection of rules, and a policy set is made up of policy sets and/or policies. A social device in an IoET device social network must restrict access to data and services to devices with a certain kind of social connection, social similarity, degree of trustworthiness, social activity, frequency of social contact, and length of social contact. Consequently, it is essential to represent these social limitations as XACML access restrictions. Social device attributes include resemblance, trustworthiness, and social activity. In XACML, they may thus be represented as either characteristics of the requested device (i.e. resource) or attributes of the access requester device (i.e. subject). However, neither device characteristics nor contextual factors can adequately describe the kind of social interaction, frequency of social contact, or length of social contact. The social connection between two social devices is described by these social properties.

Furthermore, the declaration of social connection limitations as access control needs is not supported by the XACML standard. It would be interesting to respond to the following query in order to resolve this issue: How can the XACML policies be updated to include the social connection features? Additionally, an instructor must let student devices to communicate with classroom-deployed

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp1074-1082 Vol. 21, Issue 2, 2025

equipment in order to provide an interactive course. For example, the instructor must temporarily give the chosen student's tablet his "write" permission so that the student may participate in the class and write on the whiteboard. The chosen tablet writes responses on the smart whiteboard using the authorisation that has been given. In this instance, a delegation action is used to get the access authorisation. The process by which a delegator temporarily or permanently passes all or a portion of his own access rights to a delegatee, assuming he has the authority to do so, is known as delegation. To regulate the delegation process, a delegation policy model [19] specifies both the contextual and delegation criteria. The social characteristics of the delegator, the delegatee, and their social connection must be included as social requirements in order to create the delegation regulations that govern the delegation process. This is similar to access control. As a result, we must use a delegated policy model that facilitates the articulation of these social criteria.

II. LITERATURE SURVEY

"The creation of a smart campus: An overview and conceptual model,"

T. Washington, M. Limb, T. Yigitcanlar, and K. Polin,

A new idea made possible by potential for digital transformation in higher education is the "smart campus." In addition to its conventional teaching, learning, and research roles, smart campuses are sometimes seen as smaller versions of smart cities and act as living laboratories for the creation, adoption, and study of smart technologies. The idea and implementation of the smart campus are now poorly understood. Using a systematic literature review that adheres to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology, this research fills this gap. The study categorises previous research using the four primary categories of the smart campus: society, economics, environment, and governance. Each of these areas is in line with the core ideas of big data and digital technologies on smart campuses. Little evidence of a thorough real-world implementation of the smart campus that addresses all four domains was uncovered during the investigation. This demonstrates how young the present theory and methodology are. Through a conceptual framework, the results inform the practice of the smart campus idea and help to establish a new conceptual base and research objectives. In addition to offering a solid foundation for a thorough conceptualisation of smart campuses, the results presented in this study also give guidance for further smart campus research and development.

"Intelligent education and emerging trends,"

J. C. R. Fernandez, J. A. Ruiz-Vanoye, A. Ochoa-Zezzatti, R. A. Barrera-Camara, F. R. Trejo-Macotela, O. Diaz-Parra, A. Fuentes-Penna, and J. Rodriguez-Flores,

Combinatorial optimisation, machine learning, big data, data visualisation, the Internet of Education Things, learning analytics, and other technologies are all used in smart education to improve the quality of instruction. To put it another way, smart education is the process of managing technical, financial, and human resources from research facilities and educational institutions as efficiently as possible. The Smart Society, which is a component of a Smart City, includes Smart Education. The Internet of Education Things (Wireless Sensor Networks, RFID Technology), infrastructure management, smart classrooms, smart campuses, smart learning, learning analytics, smart analysis, data science, education impact, and educational policy are the components of smart education. By providing an overview of the traits, taxonomy (education-hard issues and education-soft problems), smart education

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp1074-1082 Vol. 21, Issue 2, 2025

indicators, history, and upcoming developments, this article serves as a guide for comprehending the components of smart education.

"Security risks associated with social Internet of things in higher education,"

N. E. M. Khalifa, M. H. N. Taha, and A. A. Mawgoud,

The social internet of things (SIoT), a new wave of rapid-growth change that started and is expected to spread with more potent connectivity and interoperability of diverse devices, has proven advantageous in the trials of technology utilisation for society. This emerging IoT paradigm involves unique IoT devices interacting and forming connections with one another in the academic sector. In an objective manner, objects are forming their social connections. Understanding how social IoT items may interact with higher education systems in order to develop a safe system is the primary challenge. Thus, concentrate on the models of trustworthiness. There may be a significant danger of identity and information leakage, device manipulation, records fabrication, server/network assault, and consequent impact on application platforms due to the billions of connected devices. The range of networked devices in the academic learning sector is constantly expanding, but so are the many security risks and weaknesses that these gadgets at universities face. One of the most important technical issues facing the Internet of Things today is security. Device security, data transmission security, data storage security, and security inside systems and applications are only a few of the numerous facets of security. Although there is a vast amount of literature on the matter with many problems and answers, the majority of the works that are now available do not provide a comprehensive perspective on protection and data privacy concerns in the Internet of Things. This study's main goal is to outline the risks and threats that SIoT faces by determining (a) the key areas in which SIoT is heavily utilised in higher education, (b) the security requirements and difficulties that SIoT is currently facing, and (c) the security solutions that have already been proposed or implemented along with their drawbacks.

"A review of the opportunities and challenges of the Internet of Things (IoT) in education,"

According to M. Al-Emran, S. I. Malik, and M. N. Al-Kabi, the Internet of Things (IoT) is the most difficult platform for predicting how physical things will correlate in the near future. The utilisation of IoT and its applications across several areas have been analysed and synthesised via a broad range of review studies. A thorough overview study on the use of IoT in education is, however, lacking in the literature. Thus, this study's primary goal is to draw attention to the recent advancements in the use of IoT applications in education while outlining a number of potential and difficulties for further research. The potential for implementing IoT in education, medical education and training, vocational education and training, green IoT in education, and wearable technology in education are all summed up in this review research. It is determined that IoT adoption and uses in poor nations are still in their infancy, and further study is strongly advised.

"Smart-its friends: A method that allows users to quickly connect smart artefacts,"

F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, H. W. Gellersen, L. E. Holmquist,

The idea that everything is interconnected is linked to ubiquitous computing. Nevertheless, the quality and use of connections—rather than their quantity—will be crucial for the emergence of successful applications. Our focus is on how users may maintain control over artefact interconnection while establishing qualitative relationships and more selective linkages amongst smart artefacts. Using the context of artefacts for matching, we suggest context

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp1074-1082 Vol. 21, Issue 2, 2025

proximity for selective artefact communication. We also recommend giving consumers easy-to-use tools to force the same context on many objects. We have used Smart-Its Friends, which are tiny embedded gadgets that link when a user holds them together and shakes them, to demonstrate our argument.

III. SYSTEM ANALYSIS & DESIGN

EXISTING SYSTEM

For safe service and data exchange, access control systems are essential. For SIoT systems, SocIoTal [17] uses an authorisation mechanism based on the XACML standard. However, the social limitations in the access control policy formulation are not taken into account by the XACML standard. The adaptive fine-grained access control [21] uses a game theory technique to calculate the interest similarity to give access and exploits the similarity of social links to include the social needs into the authorisation process. However, this process does not take into account aspects like trustworthiness, contact frequency, and length that might influence the access choice; instead, it merely incorporates the kind of social connection and interest similarity as social qualities to create an access decision. Furthermore, the contextual variables used to assess the access request are not integrated.

OASIS has suggested a standard called eXtensible Access Control Markup Language (XACML) [16]. It is used to put the authorisation system into place and specify the access rules. It consists of two primary components: (1) the data flow model, as shown in Fig. 2, and (2) the policy language model, as shown in Fig. 1. The five entities that make up the XACML-based authorisation mechanism, as shown in Fig. 2, are suggested in the XACML standard [16]. The authorisation decision is enforced by the Policy Enforcement Point (PEP), which intercepts the access request. Messages between various entities are coordinated by the Context Handler (CH). The access policy established is stored and managed by the Policy Administration Point (PAP). The contextual information's source is the Policy Information Point (PIP). After comparing the access request with the access policy established and contextual data, the Policy Decision Point (PDP) gives the PEP an authorisation decision.

The data flow model, which depicts the series of communications sent between various authorisation mechanism components, is shown in an existing system [27]. The PEP receives a request from an access requester in accordance with the XACML method [16]. The subject (i.e., the person making the request), the resource to be accessed, and the action to be taken are all included in the access request. The CH receives the request from the PEP. To determine if the access requester has the necessary authorisation, the CH first forwards the request to the PDP. The PDP asks the PAP to get the requester's access policy set from the policy database. When the access policy set is located, the PDP asks the PIP (via the CH) for the contextual data. The PDP then compares the access request to the contextual data and the access policy set, and then sends the access decision back to the CH. The authorisation decision is sent to the PEP by the CH.

Disadvantages

A Social Internet of Things platform for educational institutions known as the EducationalSIoT platform is not implemented in the current system. The foundation of our EducationalSIoT platform is an application-specific blockchain.

PROPOSED SYSTEM

• We go over the social characteristics and show how they are currently categorised. Next, we

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp1074-1082
Vol. 21, Issue 2, 2025

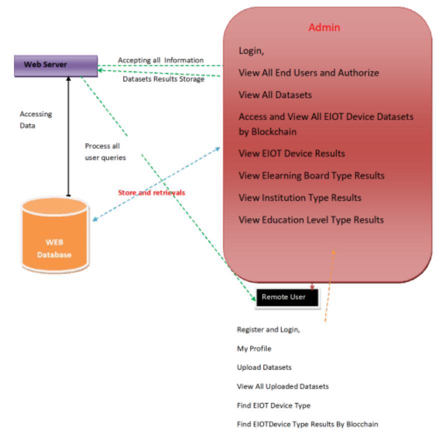
suggest additional categories according to the feature's kind, dynamicity, and nature.

- As an application-specific blockchain, we suggest an Educational Social Internet of Things (EducationalSIoT) platform [20]. To the best of our knowledge, no work has yet to propose an educational platform built on the application-specific blockchain technology and the social network of IoET devices.
- Class Object Relationship (ClsOR) and Institution Object Relationship (InsOR) are two new forms of social connections that may be established in an academic setting in order to adjust social relationships to the functions and activities of IoET devices in an academic institution.
- In order to define the social constraints necessary for making an access choice or a delegation decision, respectively, we expand the XACML policy model and suggest a delegation policy model. We make the necessary changes to the data flow models and the policy assessment procedures based on the suggested policy models.
- We advocate giving rules and policies a priority in order to provide access and carry out delegation operations in emergency scenarios. We also offer novel priority-based combining algorithms to determine which rule or policy has the greatest priority for access or delegation.

Advantages

- ➢ One may categorise the social elements as either dynamic or static. In contrast to dynamic social characteristics, which may alter their values based on time, device location, or social context, static features are immutable.
- ➢ A social feature may be a feature of the social connection or a feature of the social gadget. The social characteristics of the device define the social device, and the social characteristics of the relationship define the social connection between two social devices.

SYSTEM ARCHITECTURE



IV. IMPLEMENTATION

Modules

Admin

The administrator must use a working user name and password to log in to this module. He may do many tasks after successfully logging in, including seeing all end users and authorisingSee Every Dataset,View and Access Every EIOT Device Dataset via BlockchainView the Results for EIOT DevicesView Results by Elearning Board Type, Institution Type, and Education Level Type.

View and Authorize Users

The administrator may see a list of all registered users in this module. Here, the administrator may see the user's information, like name, email, and address, and they can also grant the user permissions.

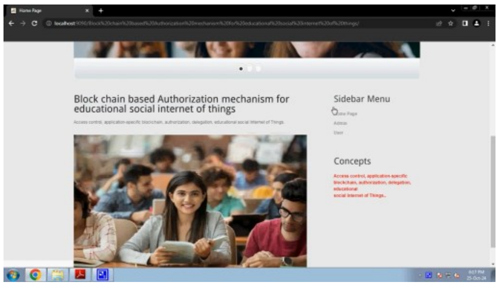
User

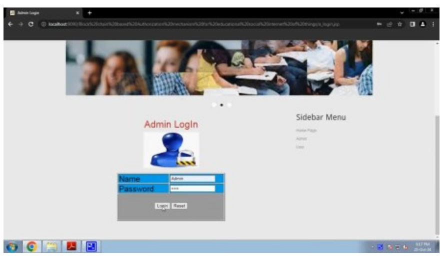
A total of n users are present in this module. Before beginning any actions, the user needs register. Following registration, the user's information will be entered into the database. Following a successful registration, he must use his password and authorised user name to log in.

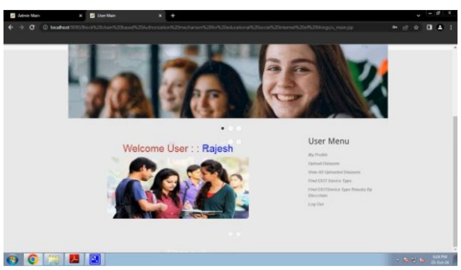
International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp1074-1082
Vol. 21, Issue 2, 2025

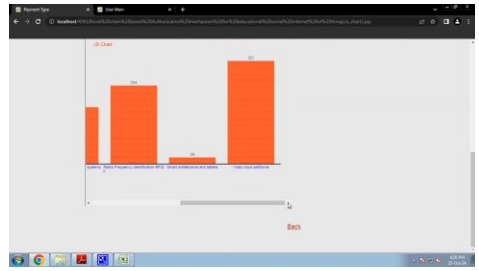
Following a successful login, the user may do several tasks, such as registering and logging in, seeing all uploaded datasets, uploading datasets, finding EIOT device type, and finding EIOTDevice type results by Blocchain.

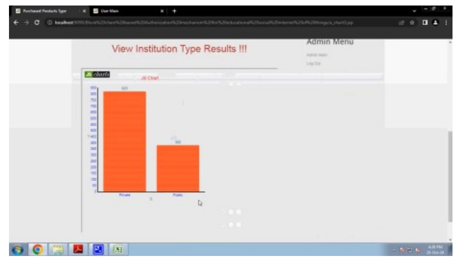
V. RESULTS

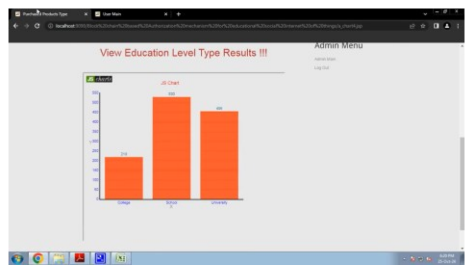












VI. CONCLUSION

In order to provide academic services based on the social network of IoET devices, we present in this study an Educational Social Internet of Things (EducationalSIoT) platform. In order to effectively deliver academic services for many stakeholders, including instructors, administrative personnel, and students—especially students with disabilities—our EducationalSIoT platform makes use of the social interactions inside the classroom and the institution. We include the social circumstances in the XACML policy model to protect the shared data and information. By modifying the policy assessment procedure and putting forward new rule-based and policy-based combining algorithms, we expand the XACML authorisation mechanism. Additionally, delegation procedures may assure the access permissions. Therefore, in order to regulate the

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp1074-1082 Vol. 21, Issue 2, 2025

delegation process, social restrictions are included into the access authorisation delegation procedure. According to the simulation findings, our access control mechanism's scalability and performance are guaranteed by the processing times for policy and request assessment. We also guarantee the security of our EducationalSIoT platform against replay and man-in-the-middle attacks, as well as the confidentiality and integrity of the data supplied by the academic services. In order to include students with disabilities into the learning process, we propose expanding our EducationalSIoT platform in the future by including additional services like the smart disability aid services. Additionally, based on the Friend of A Friend (FoAF) social interactions, we want to include the social characteristics to carry out indirect delegation operations.

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

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp1074-1082
Vol. 21, Issue 2, 2025

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 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