Grenze International Journal of Engineering and Technology, January Issue

A Machine Learning-based Framework for Monitoring and Mitigating Unauthorized Access in Computer Networks using Apache Web Logs

Meghana Lokhande[1], Rupesh Poudel[2], Ghanashyam Puri[3], Sameer Khatiwada[4] and Roshan Yadav[5]
[1-5]Department of Computer Engineering, PCCOE, Pune
Email: meghana.lokhande@pccoepune.org, rupesh.poudel22@pccoepune.org, ghanashyam.puri22@pccoepune.org, sameer.khatiwada22@pccoepune.org, roshan.yadav22@pccoepune.org

***Abstract*— Security of dynamic networks depends on access control, yet this security approach struggles to meet modern IoT and M2M demands. The proposed framework unifies Machine Learning anomaly detection with Blockchain decentralized authentication and Zero Trust security models. Dynamic permission management together with real-time threat detection produces a framework that delivers reliable, adaptable, and scalable access controls. Security operations within industries including smart cities, healthcare, and industrial automation benefit from the system's capabilities.**

***Index Terms*— Access Control, Machine Learning, Blockchain, IoT Security, M2M Communication, Attacker-Resistant Mechanisms, Zero Trust Architecture, Anomaly Detection, Behavioral Analysis, Decentralized Authentication, Dynamic Permissions, Cybersecurity, Smart Cities, Healthcare Automation, Distributed Systems.**

I. INTRODUCTION

Through the fast expansion of Machine-to-Machine (M2M) networks, industries experience industrial transformations thanks to device autonomous communications capability. M2M communication brings efficiency improvements while driving innovation across smart manufacturing and healthcare alongside logistics and various other application domains. The conventional access control systems based on static centralized designs fail to tackle M2M networks which demonstrate distributed characteristics and dynamic operational patterns.

The core function of modern cybersecurity depends on access control to verify authorized entities for sensitive re- source exchange. RBAC alongside ABAC access-control pat- terns function well under stable administrative circumstances through role and rule enforcement yet fail to fulfill current system needs that involve real-time communications alongside changing human interactions.

The authors address the existing limitations of the frame- work by integrating attacker-resistance factors with the help of the Machine Learning analytics and inclusion of blockchain in M2M access control architecture. The ML biometric data analysis methods develop techniques that combine historical and real-time data elements in administering adaptive permissions and detecting abnormalities during security threat recognition. ML-systems capable of tracking the activities of the user and modulating security controls based on environmental changes and offering immediate safety allow end-to-end threat mitigation.

Grenze ID: 01.GIJET.12.1.89

The framework attains the improved performance with the use of blockchain technology that allows the decentralized authentication and eliminates the reliance on central author- ities. The blockchain technology facilitates secure automated access control having situational awareness capability through its tamper-evident ledger and its smart contract operations.

The security framework becomes stronger when using attacker-resistant mechanisms including Zero Trust architectures which force strict verification access at all points. The method creates strong defenses against future cyber threats by minimizing security weakness points.

This article proves that there is an integrated approach to improving M2M network security with the help of the latest technological systems. The study will see the redesign of the existing access control systems by developing and implementing more flexible systems with powerful capabilities. By combining the real-time adaptive technology founded on ML with decentralized security provided by Blockchain and mechanisms of adversary degradation, the proposal allows having a full-scale solution to the M2M network protection against modern threats.

II. Literature Review

Access control security in Machine-to-Machine (M2M) networks has received a lot of attention, particularly due to the inclusion of Machine Learning (ML), Blockchain, and mechanisms that resist attacks. These technologies provide a hopeful resound to improve on security, to counter the weaknesses and to curb risks that may arise because of unauthorized access in the decentralized systems.

The use of Machine Learning to enhance access control sys- tems has recently been studied. Earlier machine learning-based approaches, including the one proposed by Hays and Efros (2008) adapted access control systems to the changing environ- ment, and used the decision-tree algorithm to categorize access requests and modify permissions according to the changing patterns.

These systems however were based on fixed models which restricted scalability on high velocity M2M networks. Masone and Caputo (2021) suggested a transition to adaptive ML-based systems and pointed out the reinforcement learning and anomaly detection as examples of methods used to identify unauthorized access attempts. Such systems constantly check the user behaviors and modify permissions in real time thereby improving security [1], [2].

Blockchain technology has also been considered to de- centralize and provide access control in M2M systems, and it might be secured. Weyand et al. (2016) presented an example of how blockchain may provide tamper-resistant and decentralized authentication and authorization, eliminating the usage of central authorities and minimizing the risk of attacks such as spoofing. Despite this merits, blockchain may prove to be resource and cumbersome, which can lead to latency and it is hard to address real time applications. Additionally, De Fontnouvelle (2021) revealed how it is possible to integrate blockchain to access control systems of the IoT to offer the integrity and traceability of access logs. Scalability however is an issue with large amounts of real time data [3], [4].

It is necessary to include attacker-resistant mechanisms into the access control systems to deal with more advanced cyber threats. According to Ranjan et al. (2016), the concept of zero trust architectures implies that devices and users should be continuously verified, and the network location or the prior authentication should not be implicitly trusted. Although this model is a great improvement in terms of security, it poses the challenge of integration particularly to the old systems. Subsequent studies by Bingel and Sokgaard (2017) showed that Zero Trust is better applied in conjunction with the ML- based anomaly detection to offer a multi-layered security system that can offer more resistance to the advanced attack techniques such as spoofing and privilege escalation [5], [6].

Hybrid access control systems offer a dynamic solution to security by integrating the traditional models (Role-Based Access Control (RBAC) and ML techniques). It has been demonstrated that when used alongside RBAC, ML can work to improve the decision making process through providing context-based and adaptive permission changes. Such a hybrid model enhances the granularity of access control, which is the inflexibility of traditional systems and which adapts the latter to changing M2M environments. Nonetheless, although ML has the capacity of optimizing security through adaptation to the varying conditions, it also demands a lot of resources when it comes to the training and deployment [7].

In summary, it has been indicated by recent literature that it is necessary to have more adaptable and decentralized access control mechanisms. Implementing ML, blockchain, and Zero Trust principles have demonstrated their potential in improving security, but the issues of resources usage, the connection with legacy systems, and scaling need to be resolved to help these technologies be viable in actual M2M settings.

A. Common Findings from Literature Review

Most Used Datasets

Centralization vs. Decentraliza- tion: The classical access control systems like Role-Based Access Control (RBAC) in most instances have central systems that serve as single point of failure and are therefore prone to attacks. The decentralized structure of blockchain, on the other hand, spreads control and gets rid of this threat, making it safer and less likely to have data breaches. As noted by Almufleh et al. (2022) and Kim et al. (2023), one of the aspects of access control that can be used to boost security is decentralization [1], [2].

Scalability Issues: Systems that use blockchain have been known to create problems with scalability in the context of IoT devices, which have minimal computing capabilities and storage capacity. To overcome them, scholars such as Liu et al. (2023) and Zhao et al. (2024) suggest hybrid solutions, which are a combination of blockchain and lightweight consensus algorithms, which would guarantee enhanced scalability in IoT networks with limited resources. [3], [4].

Most Used Evaluation Parameters

Real-Time Decision Making: One of IoT's primary obstacles to real-time decision making is latency brought on by the blockchain's transaction verification process. As demonstrated by Li et al. (2023) and Gupta d. (2022), a number of studies recommend combining off-chain solutions or blockchain technology with machine learning (ML) algorithms to increase the effectiveness and flexibility of decision-making [5], [6].

Data Integrity and Transparency: This is one of the most valuable advantages of the technology as the ability of blockchain technology to provide indelible data which ensures the integrity of information in IoT systems. This is used to ensure the exchange of actions and data of devices in the IoT is transparent and unaltered so that there is trust in the devices, users and administrators. This is supported by Wang and Choi and Kim (2022) [7], [8].

Other Notable Findings

- Decentralization: Decentralization of access control in distributed networks through blockchain and trust-based systems is typically used to give enhanced security in M2M and IoT settings.
- Scalability: The old access control models are not com- patible with large scale M2M network and hence the interest in the dynamic or attribute based access control mechanisms as a way of scaling.
- Trust and Interoperability: The models based on the trust are required in the evaluation of the reliability of the devices, and the interoperable approaches are important to communication in the heterogeneous networks.
- Security and Privacy: The security and privacy of IoT devices continue to be a priority, and solutions have been developed to ensure that these devices are not accessed by unauthorized parties and that the data is not compromised.
- Dynamic and Efficient Access: The systems need to be dynamically responsive to the modification of the conditions and guarantee resource-effective access control, particularly when environmental conditions are quickly changing in the IoT environment.
- ML-based Adaptability: Machine Learning (ML) sys- tems are highly beneficial in improving the flexibility of access control systems through real-time decision-making and constant monitoring.
- Behavioral Analysis: Behavioral analysis is a central area that can be used to detect and eliminate insider threats and enhance general system security.
- ML Model Integration: To implement the ML models in interaction with the access control mechanisms, the data preprocessing is necessary to make them compatible with the security measures and increase the detection rate.
- Anomaly Detection Accuracy: The problem of FMS has been tackled by advanced ML algorithms that prove to be highly accurate to detect anomalies and unauthorized access attempts, which strengthens the trustworthiness of access control systems.

III. PROPOSED METHODOLOGY

Machine learning, blockchain technology and decentralized identity management are some of the advanced methods that have been considered in this solution to address the issue of access control in the IoT and M2M environment.

This framework brings together M2M communications, anomaly detection based on machine learning, and decentralized access management based on blockchains to enhance the security, scalability and real-time decision-making in IoT networks. The way of how it is done is divided into several key stages: M2M

authentication, device life cycle management, secure communications, dynamic access control and system optimization.

A. Decentralized Access Control based on blockchain

The mechanism of issuing a new access control system based on blockchain technology is decentralizing access per- mission and management, which may minimize the possibility of centralized failures. The transparent and immutable nature of blockchain enables access logs to be immutable and thereby building trust among the devices, users and administrators. The identity and access credentials of each device get stored on the blockchain and cryptographic techniques provide assurance of the integrity of the data stored and authentication measures. This decentralized model reduces the chances of data breach and unauthorized access that are constant in traditional, cen- tralized systems of access control.

B. Scalability and Resource-Efficient Access Control

Blockchain has found application in the IoT that has made it use masks of hybrid models that integrate blockchain with lightweight consensus algorithms like POA and DPoS due to the limitations on the application of blockchain. The algorithms minimize computing and resource needs and every resource-constrained devices can be involved in the network without severe deterioration in performance. The system dy- namically adapts the access control protocols depending on the type of device and resources available in the system to make sure that it works efficiently with a broad range of IoT devices and network conditions.

C. Machine-Learning Based Dynamic Access Control

Machine learning (ML) is essential in real-time access control decision adaptation. It also employs special hardware to identify abnormal behaviour of the users behaviour and their traffic in the network. This enables access control which varies according to real-time information and circumstances to ensure that devices are granted or denied access according to their behavior and the prevailing circumstances in their environment. The system constantly trains its ML models on new threat intelligence in order to keep the accuracy and usefulness of access control decisions. Moreover, behavioral analysis is used in order to identify insider threats, as well as in preventing the unauthorized access of compromised devices.

D. Machine-to-Machine (M2M) Communication and Device Authentication

M2M communication integration is a major factor in se- curing and automating the process of interaction among IoT devices. Decentralized identity management (DID) is used to authenticate devices in M2M communication in this system using cryptographic keys. Devices can also connect through lightweight protocols like MQTT and CoAP that are optimized to work with IoT environments and provide secure and effi- cient data flows at low bandwidth usage. TLS/SSL encryption is used to make sure the end-to-end security of data during transit.

- M2M Authentication and Authorization: Individual M2M devices are secured with proper cryptographic protocols such that access to the network is only availed to established trustworthy devices. DID systems with blockchains authenti- cate the identity of the device and then proceed to interact with other devices in a trusted communication environment. The system proposes the implementation of a mechanism known as role-based access control and machine learning models that vary the permissions in the wake of how the devices behave and the context in which they are being used.
- Smart Device Communication Protocols: The protocols used to facilitate effective M2M communication in the system include MQTT and CoAP. These are light weight commu- nication protocols, which believe that devices can exchange data in a fast and secure manner. Integrating these protocols along with encryption techniques is one of the key elements of the system which eliminates man-inthemiddle (MITM) attacks and makes sure that no information is transferred between the devices without being compromised.
- Real-Time Decision Making and Access Control: M2M needs real-time decision-making. Our suggested system relies on machine learning algorithms to keep an eye on commu- nications done by the device and activity in the network. Any behavior that is out of the ordinary i.e. occurring of unauthorized access attempts or unusual data patterns triggers an immediate change of the device access permissions. The system employs edge and fog computing to compute the data on site and minimize the latency and achieve prompt response time on real-time access control decision-making.

E. Secure Device Lifecycle Management and Smart Contracts

Secure registration and regular updates on blockchain-based smart contracts allow the process of the lifecycle of M2M devices, i.e. onboarding to decommissioning. Such contracts are verified formally to make sure that no vulnerabilities abide in these contracts before implementation. The smart contracts have trusted oracles that

modify the security protocols as per the changing network conditions and threats. Also, the system can be upgraded to accommodate the new security challenges through upgradable contracts, which would ensure that the IoT devices are constantly safeguarded against emerging threats.

IV. ALGORITHMS

Following is a description of the important algorithms required.

A. K-Means Clustering

K-means clustering is one of the most famous machine learning algorithms to cluster similar data points. In terms of access control, it is useful in determining the patterns of user behaviour or access requests by grouping users with similar characteristics or access patterns. As an illustration, one can apply this algorithm in clustering users according to their frequency of access, time of access, or location in order to indicate the outliers or suspicious access that does not follow the pattern. K-means clustering finds its applications in M2M where anomaly detection is possible in a large scale system.

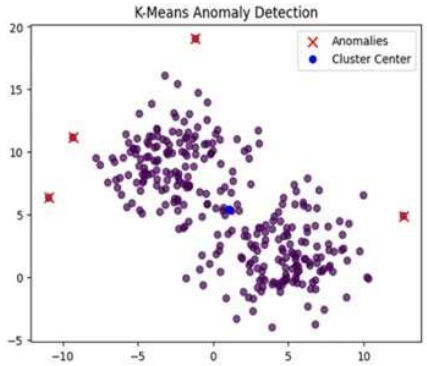

Fig. 1. Illustration of K-means clustering for user access patterns in M2M networks.

The major strength of K-means clustering is that it is efficient particularly when handling huge volumes of data. It is capable of functioning in an unsupervised fashion, that is, its operation does not need labelled data, and therefore it is very flexible to the dynamics of M2M environment. The algorithm is however prone to difficulty when handling complex, high- dimensional data, that might need a very keen feature selection and preprocessing.

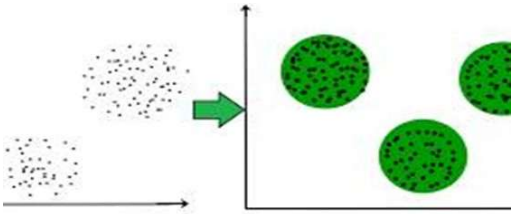

Fig. 2. Working mechanism of K-means clustering algorithm.

B. Random Forest

The Random Forest technique of ensemble learning is more effective in terms of accurate prediction with the use of mul- tiple decision trees. It is especially useful in the classification of access requests as legitimate or as suspicious access control systems. Random Forest may be used to identify a new request as acceptable or not by comparing the historical data (access requests and user behavior). The algorithm is resistant to overfitting, and, therefore, it can be highly accurate even when the data is massive and contains many noise points, which makes it suitable to real-world and complex scenarios, such as the M2M networks.

Random Forest is applicable to M2M access control as access pattern and malicious intention can be observed with the help of this method (unauthorized access, attempts to break security measures, etc.). Random Forest has the merit that it can work with both categorical and numerical data and thus will be very useful in very diverse security-related activities.

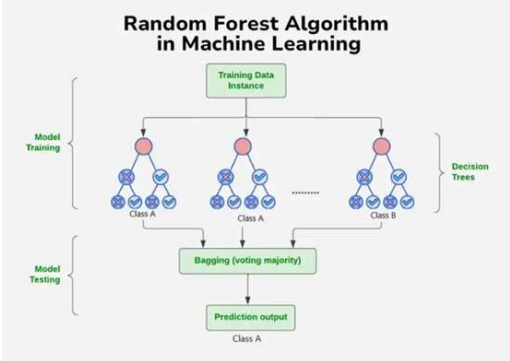

Fig. 3. Random Forest ensemble method for access control classification.

C. Role-Based Access Control (RBAC)

One of the most popular models of the access control is Role-Based Access Control (RBAC), which is among the access control models used in large scale distributed systems.

RBAC assigns permissions to roles and not to an individual user or device and a user is then granted access according to his role. This makes it easier to control the permissions par- ticularly in organizational setups that have numerous entities and users.

RBAC is an important role in M2M networks where it assigns roles to machines or devices depending on the functions which could include sensors, actuators or controllers. This enables an easy access management, because similar devices of a position share a similarity in access control. However, RBAC is not applicable in dynamic environments like in the IoT where devices may require different permissions under different circumstances of the context like location, time or security clearance. This has seen the consideration of more dynamic models like the Attribute-Based Access Control (ABAC) due to the rigidness of the RBAC.

Fig. 4. RBAC architecture and role hierarchy

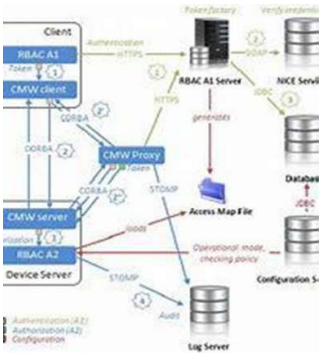

Fig. 5. RBAC access control workflow.

D. Attribute-Based Access Control (ABAC)

Attribute-Based Access Control (ABAC) is an extension of RBAC which takes into account other factors other than user roles. Access decisions in ABAC are reached by a combination of user, device and environment-related attributes. Attributes may be user identity, device type, time of access, location or security clearance and provide fines control over access permissions.

The first strength of ABAC is its flexibility and adaptability especially in contexts such as M2M and Internet of Things networks where contextual information is highly important. As an example, a sensor can be able to access certain resources with limited hours or even a specific place. This is because by including a variety of attributes, ABAC will be able to dynamically change permissions in real-time, increasing the security of the M2M systems so that only under the circumstances the access is granted.

Nevertheless, ABAC is complicated in regards to man- agement and implementation since it will demand effective systems in evaluating and storing attributes. ABAC is very appropriate to large distributed systems that have inadequate role-based access systems irrespective of these obstacles.

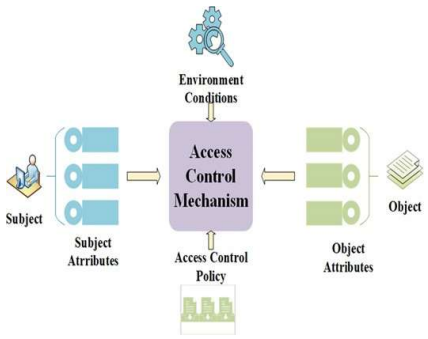

Fig. 6. Attribute-Based Access Control model architecture

E. Artificial Neural Network (ANN)

Artificial neural networks (ANNs) are computer programs based on human brain that discover patterns and formulate their decisions by referring to data. ANNs are dynamic and adaptive, in the sense that they learn typical access patterns and discover deviations as possible security threats in access control. Unlike the traditional systems where Role-Based Access Control (RBAC) is a system where access is granted to users based on the role they are assigned, ANNs take into account other parameters such as access behavior of the user, security of the device, place and time so as to make decisions of access based decisions. This gives more flexibility in control and real-time.

ANNs have great benefits as compared to RBAC. Whereas, RBAC cannot be applied to dynamic environments, as it is restricted by predefined roles, ANNs are capable of continuous learning and adaptation to new patterns without a manual update. ANNs can be used in detecting anomalies as well based on the user behavior and this provides better defenses against unauthorized access. Also, ANNs are more scalable in a complicated environment, and they can adapt to access depending on the risk characteristics in real time, whereas RBAC can become bulky when the number of roles and permissions grows.

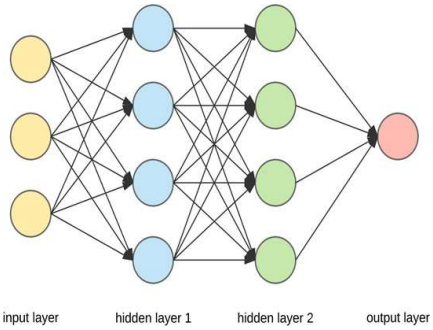

Fig. 7. Artificial Neural Network architecture for access control.

Overall, ANNs offer a stronger, scalable, and adaptable access control mechanism that has better performance than the traditional RBAC in providing context-aware and risk-aware decision-making capabilities and anomaly detection to achieve security.

F. Smart Contract for Decentralized Access Control

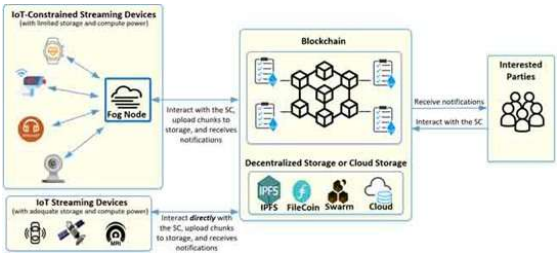

Fig. 8. Illustration of blockchain-based smart contract for decentralized access control.

Smart contracts are central units that are used to achieve decentralized access management by automating permission and guarding it against central authoritativeness. Blockchain- based smart contracts are used to implement predetermined rules of access rights and offer immutability and transparency combined with operational trust. Their immediate authentica- tion systems coupled with their dynamic permission handling reduces the risks of data leakage and illegal system access by the internal staff. Intelligent contracts to the decentralized access control systems allow network expansion and speed of operation to be effective, in particular in the IoT and M2M systems of complex networks. The access control methodology developed by Logchain provides rapid authentication with audit trailability and resistance to cyber-attacks to secure systems with the highest level of security that are needed in such industries as finance, healthcare, and smart infrastructure.

G. Role-Based Access Control (RBAC) with Blockchain for Internet of Things

SunlightBracketAccess (RBAC) with blockchain systems provides secure and efficient approaches to managing access control needs in the IoT networks. RBAC App access man- agement with Click app is an access control mechanism that enables users and devices to be authenticated by utilizing pre-defined roles upon accessing IoT resources. The use of blockchain enables RBAC to meet decentralized authentication and get immutability when making accesses as well as gaining access logs and transparent access events. Blockchain does not require the supervision of a central authority, which decreases the network points of failure to enhance IoT safety. The tamper-proof features of blockchain help organizations to defend themselves against internal attackers and unautho- rized access since access control policies and logs cannot be modified. The integrated system is most efficient when working on dynamic IoT environment environments that rely on scalability of operations coupled with real time validation of secure device communication in smart homes, automation in industries and medical systems.

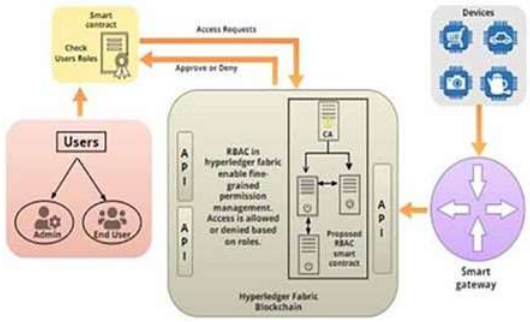

Fig. 9. Integration of RBAC with blockchain for secure IoT access control.

V. Conclusion

The development of the IoT, M2M systems, and blockchain technologies is dynamically growing, which makes further sophisticated access control systems prerequisite. This study points to the usefulness of machine learning, decentralized authentication, Zero Trust models, and blockchain in coping with the drawbacks of the traditional access control system. Machine learning brings about the dynamic, adaptive security in which a behavioral pattern is analyzed and permissions adjusted in real-time; this can greatly improve access control within the complex environment. But issues like adversarial attacks need to be resolved to enhance the resilience of the ML-based systems.

The non-revocable and decentralized nature of blockchain makes the IoT safer as it supports the open and uncensurable process of authentication and authorization. The smart con- tracts and decentralized identities should also be integrated to increase the privacy and scalability of IoT networks, trace- ability and realtime auditing, which is critical in providing confidence in the sensitive application.

M2M requires access control to achieve safe communication and security of data integrity in the industries such as healthcare, smart cities and automation in the industries. Although the issues of scalability and capability of carrying out calculations are still a concern, the future trend of adaptive access control systems development will be the most important in terms of performance and security enhancement. The study preconditions a safer, scaled and sturdy digital ecosystem, which has a bright future in resolving the security challenges of interconnected systems as they develop.

ACKNOWLEDGMENTS

We are pleased to acknowledge our Technical Seminar- I Guide, Dr. Meghana Lokhande, who has encouraged and supported us to accomplish our seminar, in particular, the valuable suggestions made in the course of our seminar and has provided the foundation to the successful completion of this work. We are also pleased to acknowledge the support and sincere help of our Research & Innovation co-ordinator, Prof. Dr. Reena Kharat and Technical Seminar Coordinator, Prof. Bodireddy Mahalakshmi, who helped us during the initial stages of the seminar and throughout the process of conducting this seminar work. We would also like to note the assistance of Prof. Dr. Sonali D. Patil, Head of Computer Engineering Department, who granted the entire period of this seminar work. We also appreciate the assistance the teaching and non- teaching staff members to our successful seminar work. We also owe all the web communities a great deal of knowledge they have enhanced us with.

REFERENCES

[1] F. Ouaddah and H. Mousannif, ”Blockchain-Based Access Control for the Internet of Things,” Journal of Network and Computer Applications, vol. 112, pp. 43–58, 2018.
[2] Z. Xu and H. Xie, ”A Blockchain-Based Framework for Access Con- trol and Security in Cloud Computing,” Future Generation Computer Systems, vol. 102, pp. 169–178, 2019.
[3] Y. Zhang and K. Yang, ”Decentralized Access Control Using Smart Contracts,” IEEE Access, vol. 8, pp. 150873–150884, 2020.
[4] R. Singh and P. Sharma, ”Blockchain for Access Control and Autho- rization in Cyber-Physical Systems,” Sensors, vol. 21, no. 4, p. 1386, 2021.
[5] S. Aggarwal and T. Biswas, ”A Survey on Blockchain for Identity Management and Access Control,” ACM Computing Surveys, vol. 54, no. 9, Article 181, 2022.
[6] K. Ragothaman, Y. Wang, B. Rimal, and M. Lawrence, ”A Comprehen- sive Study on Anomaly Detection Techniques for IoT,” Sensors, vol. 23, no. 4, p. 1805, 2023.
[7] G. Tuna, D. G. Kogias, V. C. Gungor, C. Gezer, E. Tas¸kın, and E. Ayday, ”A Survey on the Integration of Machine Learning Techniques into Wireless Sensor Networks,” Expert Systems with Applications, vol. 86, pp. 98–114, 2017.
[8] S. Cho and B. Shrestha, ”A Study on the Performance of Wireless Communication Networks Based on the Integration of Machine Learning and Data Analysis Techniques,” Applied Sciences, vol. 12, no. 21, p. 10836, 2022.
[9] M. A. Azad, S. Abdullah, J. Arshad, H. Lallie, and Y. H. Ahmed, ”The Role of Machine Learning in Enhancing Security in IoT Devices,” Heliyon, vol. 10, no. 4, e10345, 2024.
[10] S. Ghasemshirazi, G. Shirvani, and M. A. Alipour, ”Advancements in Machine Learning Techniques for Cybersecurity Applications,” arXiv Preprint, 2023.
[11] M. M. Rooney and M. K. Hinders, ”Machine Learning for Medium Access Control Protocol Recognition in Communications Networks,” IEEE Transactions on Communications, vol. 70, no. 12, pp. 8150–8161, Dec. 2021.
[12] S. Aboukadri and A. Ouaddah, ”Machine Learning in Identity and Ac- cess Management Systems: Survey and Deep Dive,” Future Generation Computer Systems, vol. 142, pp. 112–128, Mar. 2024.
[13] A. Choudhury, M. Ghose, A. Islam, and Y. Yogita, ”Machine Learning- Based Computation Offloading in Multi-Access Edge Computing: A Survey,” Computer Networks, vol. 218, pp. 109–123, Feb. 2024.
[14] U. N. Cobrado, S. Sharief, N. G. Regahal, E. Zepka, M. Mamauag, and L. C. Velasco, ”Access Control Solutions in Electronic Health Record Systems: A Systematic Review,” Health Informatics Journal, vol. 29, pp. 1–15, Apr. 2024.
[15] K. Srivastava and N. Shekokar, ”Design of Machine Learning and Rule Based Access Control System with Respect to Adaptability and Genuineness of the Requester,” in Proc. of the 6th EAI Interna- tional Conference on Smart Objects and Technologies for Social Good (GOODTECHS), pp. 156–160, Sept. 2020.
[16] P. K. Verma and R. Verma, ”A Survey on Access Control in M2M Communications,” ScienceDirect, 2016.
[17] L. Duan, V. Shah-Mansouri, and V. W. S. Wong, ”Dynamic Access Control for M2M Communications,” PDF, 2013.
[18] S.-R. Oh, Y.-G. Kim, and S. Cho, ”Interoperable Access Control Mechanisms for IoT,” MDPI Sensors, 2019.
[19] T. Jaiswal and U. K. Singh, ”A Novel Approach to Access Control in Distributed M2M,” ResearchGate, 2016.
[20] A. Mahmood, ”Evaluation of Secure Capability-Based Access Control in the M2M Local Cloud,” IEEE, 2021.
[21] G. Shelke, ”A Blockchain Approach to Manage Vaccine Production,” Scribd, [Online]. Available: https://www.scribd.com/document/609455267/Document-1-2-merged