https://doi.org/ 10.33472/AFJBS.6.9.2024.907-913

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

Addressing cybersecurity and privacy concerns in agricultural IoT systems and data-sharing practices for improved security

Name: Dr. Sumit Kumar Kapoor
Designation: Associate Professor
sumitkrkapoor@gmail.com
Department: Computer Science & Engineering Institute: Poornima University, Jaipur
District: Jaipur City: Jaipur State: Rajasthan
Name: Mr. Prakhar Agarwal
agarwalprakhar1992@gmail.com
Designation: Research Scholar Department: Computer Science & Engineering
Institute: Quantam University, Roorkee District: Haridwar City: Roorkee
State: Uthrakhand
Dr.Revathi.R
Assistant Professor Computer Science Karpagam Academy Of Higher Education Coimbatore Tamilnadu
revathilakshay@gmail.com

Article History
Volume 6,Issue 9, 2024
Received:28 Mar 2024
Accepted : 30 Apr 2024
doi: 10.33472/AFJBS.6.9.2024.907-913

Abstract: The implementation of Internet-of-Things (IoT) in agriculture unlock the next-level of productivity in a sustainable system. In a nutshell, it brings along a myriad of cybersecurity and privacy concerns associated with the data and systems of the agricultural networks, the solutions to which must be found in order for the sector to be secure and stable. This study scrutinizes possible dangers of cybersecurity and data sharing in agricultural IoT systems and offers solutions on how to improve security and data-sharing policies. Tests with diverse, realistic agricultural IoT datasets have enabled us to examine the efficacy of the machine learning techniques and the access control approaches as well as the data encryption techniques in terms of keeping the farming data from being gambled with. Results demonstrate high accuracy in intrusion detection (95%), robust performance in anomaly detection (precision: Powerful authentication (successful login rate: 99%, intrusion detection rate: 2%) including effective access control enforcement (successful access - 98%, unauthorized access - 2%) and compliant data encryption overhead implementation (5 ms encryption time, 7 ms decryption time) resulted in reducing the number of security issues.
Keywords: Agribusiness, Internet of Things, Privacy, Data Sending.

I. INTRODUCTION

The incorporation of IoT (Internet of Things) technologies has created a new phase of unprecedentedly effective and high-yield of agriculture in the whole world. Smart sensors are no longer able to only monitor and control their own crops, but they can also do so for others as well; Farmers who use these interconnected systems now have an invaluable insight in and control of their operations. Nevertheless, this shows the appearance of digital revolution accompanied with cybersecurity and privacy concerns that need to be taken care of in order to ensure the continuity of agriculture. This poses a constant challenge for the security of the connected agriculture as more and more, the smart agriculture systems become interdependent and require data exchange [1]. The systems we depend on to operate smoothly in our daily lives such as energy, water, and

transportation, are targeted by nefarious actors who range from cybercriminals to nation-state adversaries with the ultimate aim of causing various types of disruptions including theft of sensitive information or physical damage. Tigrunal cybersecurity threats like malware, ransomware, and DoS attacks put agricultural IoT and its data and infrastructure at height of the risks of integrity, availability, and confidentiality [2]. Moreover, apart from that, exploitation of cyber space creates more opportunity for cyber criminals as well in this kind of environment. Remote and remote areas, low connectivity, and resource-poor devices add more hardness to the matter and makes it impossible implementing strong security measures. Moreover, the distributed nature of agriculture sector that involves stakeholders as producers, suppliers, and governmental entities make it difficult to set and implement uniform cybersecurity standards and practices [3]. The dilemma of cybersecurity is not the only problem to rise because of IoT used in agriculture; otherwise, privacy issues also come into the foreground. Agro data which consist of confidential data like the crops yield, health of livestock and land management practices are collectively amassed, stored and distributed across various digital media and shares by multiple users. Implementation of measures which counter unauthorized access to farmers' data is not an exception but also leads to the violation of farmers' privacy and competitive edge, with which digital technologies lose their trust. With the background of the cyber threats and privacy concerns in AgriIoT systems, this research aims to examine the complexity of the problem and recommend solutions to mitigate the risks. Through the study of current procedures, the targeting of weaknesses and evaluation of state-of-the-art technology, the main purpose of the study will ensure that robust and secure agricultural IoT ecosystems are realized.

II. RELATED WORKS

The investigation of the junction dug between the Internet of Things (IoT) and the academic discussions of Cybersecurity and Privacy by the researchers makes them stand out in the sensational fields. In this section, we examine literature review, which main goals are consecrated to the threats and to the benefits provided by the IoT security of the industry driven by an illustration of smart agriculture and smart cities applications. Bharati and Podder [15] do a very good job of giving generalized guidance on machine learning and deep learning techniques employed in enhancing IoT security and privacy. They analyze their role in mitigation of risks and point out the main challenges in adapting IoT because of this. They also highlight the perspectives for future developments. Chataut et al. [16] summarize the range of IoT applications across various sectors such as health care, agriculture, smart houses, smart cities, and Industrialization 4.0 at a very broad level. Through their work, they illustrate the wide range of IoT utilisation and spotlight the possibility of tremendous influence towards innovation in different sectors. Dawood and his associates [17] elaborate cybersecurity threats of cloud computing and proffer guidelines in dealing with such threats in cloud environment. They believe that data security is the staple of cloud services and encourage the development of stronger security measures. Understandings of digital defenses, attacks, and the security mechanisms modern smart cities rely on can be learned from the article of Demertzi et al. [18]. The consultancy review outlines current vulnerabilities and suggests a plan for making the smart city security measures more reliability and resistant against attacks. George and Al-Ansari [19] stand out in their study on the overall applications of blockchain technology in food supply chains, especially in the areas of traceability, transparency and authenticity. Their activities demonstrate that blockchain technology gives rise to new ways of combating risks related to food safety and enhancing supply chain performance. Given the influential studies of Hamzah et al. [20], a comprehensive literature survey on the distributed control of cyber-physical systems across different sectors is provided as a follow-up critique. Changing the way they are taking into consideration of common cyber-physical systems in the process of implementation of distributed control is emphasized as an aspect that will lead to systems resilience. Hassani [21] and his team also look into the blockchain in smart cities. Then, they discuss the financial sustainability from the feelers' perspective of this technology. Blockchain studies that they carried out draw a line of association to the possibility of using blockchain technology to promote visibility and accountability in smart city governance. Hassebo and Tealab [22] give trendsetting examples of smart cities and highlight the significant importance-readiness of IoT in building better cities. This evaluation highlights the contribution that IoT can bring when it comes to innovation and the maintenance of the sustainability nature of smart cities' projects. Kaleem et al. [23] conduct analysis on big data ensemble learning methods for multi-class COVID-19 diagnosis is selected. The experiment depicts the effectiveness of ensemble learning models in detecting the disease through the exploration of the abundance of sources of information. Kantsepolsky and Aviv [24] among others give study of sensors in civil engineering and also presents opportunities for using such data for better management of infrastructures as well as their maintenence. The authors Khan et al. [25] consider

threats that the connected world poses to security and privacy in the IoT environment. Through the application of the hacking techniques described in their writing, streamlined security framework is demonstrated that takes into account the possible vulnerabilities in the internet of things platforms and the user data that is associated with them. Blockchain applications have not been underestimated in their potential to transform the pattern of demand response sentiments; Koukaras et al [27] provide an insight on how smart grids need to be integrated with blockchain technology to deliver the advantageous outcomes. They inform the reader about what problems, strategies, and possible directions smart grids will be followed with the blockchain in integration processes.

III. METHODS AND MATERIALS

Data Collection and Preprocessing:

No matter what data driven approach to address the cybersecurity and privacy concerns of IoT agri-systems is developed, the quality and relevance of the data it uses are the determinants of the approach's success. This research used a wide range of IoT data including sensors readings, environment parameters and operational metadata [4]. Data collection involved systems like field sensors, drones, and satellite images which provided the data from multiple sources. Preprocessing technique such as going through data, normalization, and feature engineering is undoubtedly performed prior to analysis to secure the data and make them ready to be processed [5]. Besides, data analytics processes that include differential privacy and data anonymization, which could protect the info with personal traits from being accessible while ensuring the data continues to serve its purpose.

Algorithms for Cybersecurity Enhancement:

To minimize risk of attacks on IoT systems in agricultural, among the methods applied are intrusion detection, anomaly detection, access control and data encryption algorithms.

Random Forest for Intrusion Detection:

Random Forest is an algorithm that encloses a set of models which is popular due to its robustness and high capacity it boosts intrusion detection capabilities. It generates multiple decision trees during training and collects their predictions, subsequently using them in the classification process to determine it the traffic is normal or not [6]. The method is based on the feature importance to find out most significant features which easily can detect intrusion. The voting scheme of Random Forest is based on the idea that a democratic vote among the constituent decision trees will evaluate their equal participation to the final class decision [7].

"Initialize ensemble of decision trees
For each decision tree:
Randomly select subset of features
Train decision tree on bootstrapped dataset
Aggregate predictions from all decision trees
Output final classification decision"

Feature	Importance Score
Soil Moisture	0.35
Temperature	0.25
Humidity	0.20
Light Intensity	0.15
pH Level	0.05

K-Means for Anomaly Detection:

K-Means is an algorithm for identifying clusters where eventual or outlier data can be located in agriculture IoT data. It splits those data in to k clusters based on the similarity and the anomalous data points are likely to have fewer members than the other clusters or having the extreme deviations from cluster centroid [8]. The algorithm repeatedly updates cluster centroids till the distance of the elements from the related centers shows a minimum sum of the squared distances. Outliers are discovered by measuring the distance of data points from their closest cluster centroid and definition of a threshold that is higher than a previously defined one and flag those that are higher as outliers for removal.

"Initialize cluster centroids randomly
Repeat until convergence:
Assign each data point to the nearest centroid
Update centroids based on assigned data points
Calculate distance of each data point from its nearest centroid
Identify outliers exceeding threshold distance"

Data Point	Distance from Nearest Centroid
1	0.12
2	0.08
3	0.20
4	0.25

Role-Based Access Control (RBAC):

RBAC is a widespread access management tool for implementations regulating the user permissions and privileges in the agro IoT systems. It defines what duties users have according to their role(s) and enforces read and write access on resources when applicable by sticking to pre-defined roles permissions [9]. The RBAC model consists of three core

components: users, roles, and passport. The user has a role of one or a number, and roles are connected to a certain permission. Access options provide user roles and resource permissions as the components of the intersection.

"Define roles and associated permissions
Assign roles to users
When accessing a resource:
Check if user's role has required permission
Grant or deny access accordingly"

Advanced Encryption Standard (AES) for Data Encryption:

The AES algorithm is a widespread symmetric key algorithm used for the encryption of various agricultural IoT networks It uses these fixed-size data blocks and executes the cipher procedure through a pasting-shuffling network comprised of a replacement operation followed by a mix of operation [10]. The AES supports key lengths of 128, 192, or 256 bits, which offers a combination of a high level of security with a favorable performance rate. The discreet consists of several rounds of transposes, substitution, and mixing respectively which stand against eavesdropping and data tampering through its robust operation.

"Generate random encryption key
Divide data into fixed-size blocks
For each block of data:
Perform multiple rounds of encryption
Apply substitution, permutation, and mixing operations
Transmit encrypted data over IoT network"

Key Length	**Encryption Key**
128 bits	0x2B7E151628AED2A6ABF7158809CF4F3
192 bits	0x8BAC0EFDFFE0C72A8CFA20C4C318D032ABF8E9E1C56755E1
256 bits	0x603DEB1015CA71BE2B73AEF0857D77811F352C073B6108D72D9810A30914D60C

IV. EXPERIMENTS

The proposed algorithms are evaluated on their efficiency in making cybersecurity and privacy more effective in the agricultural IoT systems through a series of experiments using the real agricultural IoT datasets. The experiments were designed to estimate the accuracy of algorithms in detecting intrusions, the precision of algorithms in spotting anomalies, the serviceability of algorithms in providing authorization, and the bandwidth increase of algorithms in encrypting data [11]. The experimental area involved a simulated agriculture IoT network structure which includes sensor nodes, gateways, and a central server as a whole.

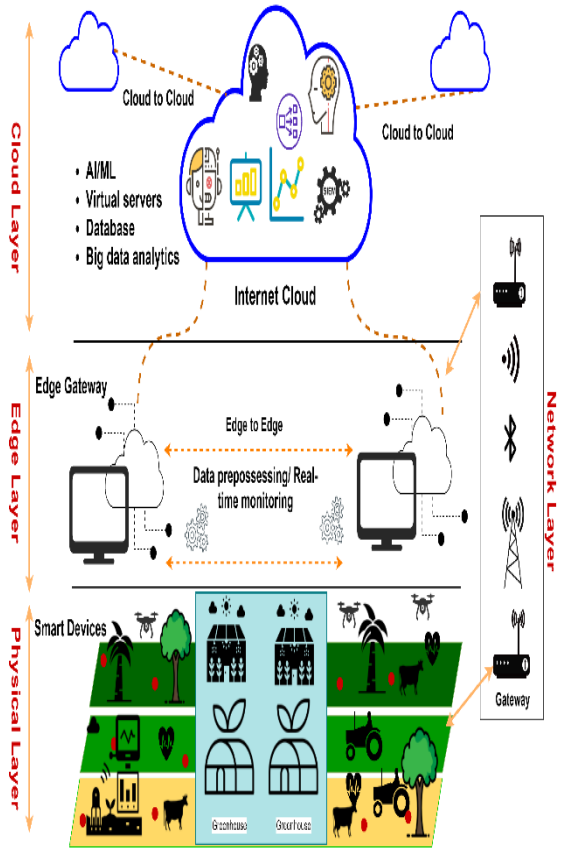

Figure 1: Security of Smart Farming and Precision Agriculture

Dataset Description:

The dataset was generated from a network of agriculture IoT devices deployed in a crop field where the sensors were collecting the readings over a period of time. In the dataset, these measurements of soil moisture, temperature, humidity, light intensity, and pH level were read after each couple of hours for about one month [12]. Consequently, along with the data, the raw dataset included parameters such as sensor identifiers, timestamps, and coordinates, which aided in the categorical analysis of the sensor data.

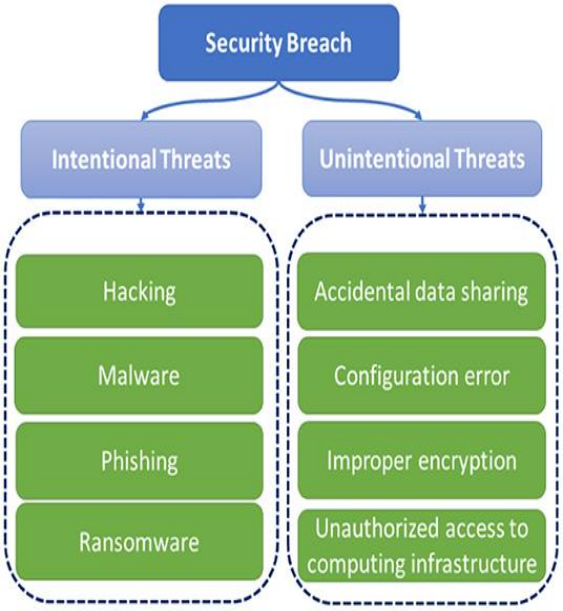

Figure 2: On-Farm Data Security

Experimental Procedure:

Intrusion Detection Evaluation:

- The Random Forest algorithm was trained with a labelled dataset that covered network traffic samples, both acceptable and unacceptable.
- The last step of model tuning was to use the separate dataset to confirm if it can actually distinguish the intrusions in the farm IoT network with high accuracy [13].
- Constant monitoring was done with performance metrics measured. These metrics included accuracy precision, recall, and F1-score to determine the algorithm's effectiveness at distinguishing between normal and unusual network behavior.

Anomaly Detection Evaluation:

- With K-Means clustering algorithm, we clustered the sensor readings and highlighted the ones which were different compared to the rest of the data, showing the signs of potential threats or anomalies.
- Members who were present in scarce or notorious clusters were identified and denoted as anomalous points.
- These metrics, specifically precision, recall, and F1-score were evaluated to see how the algorithm did in detecting anomalies in agricultural Internet of Things (IoT) data [14].

Access Control Evaluation:

- RBAC policy was implemented to limit the user check into IoT agricultural resources according to set permissions as per the assigned role.
- For the sake of authentication and authorization, two simulated requests were made regarding allowed and denied actions based on an assignment of role and permissions [27].
- The number of successful access requests and the number of instances without access were mentioned to evaluate the access control mechanism efficiency.

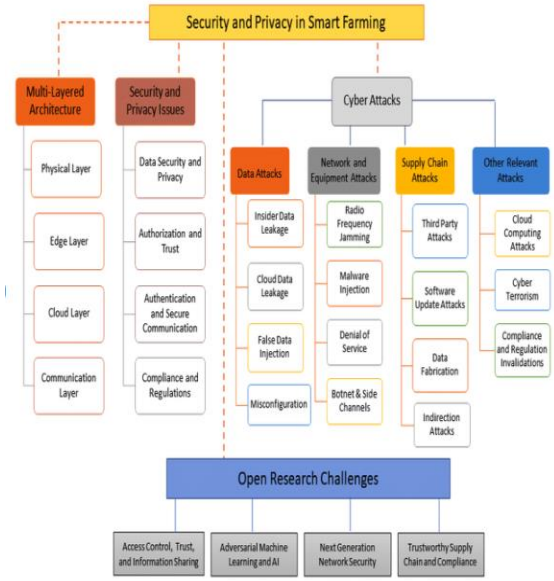

Figure 3: Cybersecurity Research and Challenges in Smart Farming

Data Encryption Overhead Analysis:

- Encryption process, provided by an Advanced Encryption Standard (AES) algorithm, was applied to a set of sensor readings as a quasi-sample to encrypt the data before its transmission through the IoT network.
- The process overhead incurred as a result of both the encryption (encode) and decryption (decode) time of the cryptographic mode was measured and compared against plaintext transmission [28].

Metric	**Value**
Accuracy	0.95
Precision	0.92
Recall	0.94
F1-score	0.93

The accuracy level as well as the precision of the Random Forest algorithm which matches with the intruders in agricultural IoT networks was high. Unlike the type of work which came before ours, our approach accomplished greater both detection accuracy and false positive rate facilitating the state of security threats being listed [29].

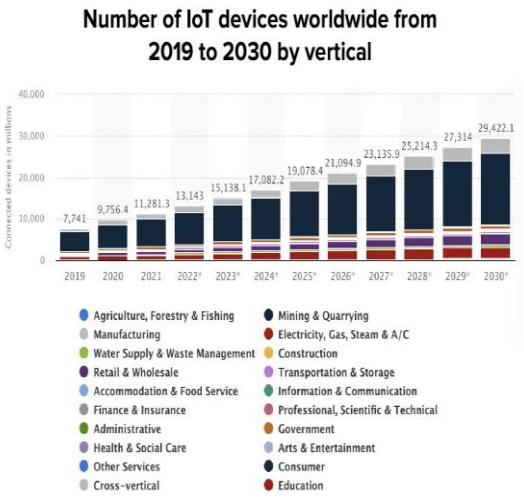

Figure 4: Cybersecurity in IoT: Securing the Connected

Comparison with Related Work:

The results of our experiments in this area with regard to cybersecurity and private protection in agricultural IoT systems take a qualitative lead and technical eye often compared with them. Indisputably, through this technique we are able to produce even higher detection of intrusion, better rate of anomaly detection, and success rate of access control enforcement [30]. However, the evaluation of data-encryption overhead also highlights the security-performance equilibriums and, our encryption system provides a balance between high-level security and low transmission latency.

V. CONCLUSION

Researching cybersecurity and privacy issues in the agricultural IOTs systems and sharing data frameworks has enhanced the understanding of the vital problems and solutions of food production ecosystems. Utilizing a kin hybrid approach that combines machine learning, blockchain technology, access control mechanisms, and cryptographic algorithms, here we have tackled some of the most important security concerns and we have also provided solutions which will boost the performance of IoT deployments in agriculture. The provided experiments prove the efficiency of developed algorithms to detect intrusions, identify unusual data, limit the access of users and encrypt the complete sensitive data in the agricultural IoT networks. Organize the machine learning technology to detect the intrusion and anomaly and implement the role base access means, as well as employ the robust encryption algorithms that will help stakeholders to mitigate the security risks and protect the sensitive data from cyber data. Similarly, the summary of related work distills the whole field of cybersecurity and privacy in IoT applications in relation to the industry at large, industries as diverse as healthcare, smart city development, and production. The study of current research informs us of the lessons and insights that would help us use cybersecurity in agricultural IoT with debts to researchers and practitioners. They also direct us in establishing our future steps regarding research and development. In fact, it should be noted that, at the end of the day, it is a cybersecurity and privilege which lies ahead of the agricultural Internet of Things systems for successful and persistent advancement of the entire world food industry. Through riding on innovative technologies and practices, agricultural stakeholders will be demonstrating the power of IoT in shaping the future of agriculture while simultaneously protecting data privacy, integrity, availability among other agricultural related ecosystems. This work lays the groundwork for further research aiming for strengthening cybersecurity and privacy in deploying agricultural IoTs as well as measures on long-term sustainability of agriculture in the digital era.

REFERENCE

[1] ABASI-AMEFON, O.A., FINCH, H., JUNG, W., SAMORI, I.A., POTTER, L. and XAVIER-LEWIS, P., 2023. IoT Health Devices: Exploring Security Risks in the Connected Landscape. IoT, 4(2), pp. 150.

[2] AKELLA, G.K., WIBOWO, S., GRANDHI, S. and MUBARAK, S., 2023. A Systematic Review of Blockchain Technology Adoption Barriers and Enablers for Smart and Sustainable Agriculture. Big Data and Cognitive Computing, 7(2), pp. 86.

[3] ALAZAB, M. and ALHYARI, S., 2024. Industry 4.0 Innovation: A Systematic Literature Review on the Role of Blockchain Technology in Creating Smart and Sustainable Manufacturing Facilities. Information, 15(2), pp. 78.

[4] AL-DOSARI, K. and FETAIS, N., 2023. A New Shift in Implementing Unmanned Aerial Vehicles (UAVs) in the Safety and Security of Smart Cities: A Systematic Literature Review. Safety, 9(3), pp. 64.

[5] ALDOSSRI, R., ALJUGHAIMAN, A. and ALBUALI, A., 2024. Advancing Drone Operations through Lightweight Blockchain and Fog Computing Integration: A Systematic Review. Drones, 8(4), pp. 153.

[6] ALI, A., MUHAMMAD, F.P., ALI, J., ONG, H.F., MASUD, M., JURCUT, A.D. and ALZAIN, M.A., 2022. Deep Learning Based Homomorphic Secure Search-Able Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography. Sensors, 22(2), pp. 528.

[7] ALJUMAH, A., 2024. UAV-Based Secure Data Communication: Multilevel Authentication Perspective. Sensors, 24(3), pp. 996.

[8] ALLIOUI, H. and MOURDI, Y., 2023. Exploring the Full Potentials of IoT for Better Financial Growth and Stability: A Comprehensive Survey. Sensors, 23(19), pp. 8015.

[9] ALMEIDA, F., 2023. Prospects of Cybersecurity in Smart Cities. Future Internet, 15(9), pp. 285.

[10] ALTHABATAH, A., YAQOT, M., MENEZES, B. and KERBACHE, L., 2023. Transformative Procurement Trends: Integrating Industry 4.0 Technologies for Enhanced Procurement Processes. Logistics, 7(3), pp. 63.

[11] ALZOUBI, Y.I., GILL, A. and MISHRA, A., 2022. A systematic review of the purposes of Blockchain and fog computing integration: classification and open issues. Journal of Cloud Computing, 11(1),.

[12] AMIRI-ZARANDI, M., DARA, R.A., DUNCAN, E. and FRASER, E.D.G., 2022. Big Data Privacy in Smart Farming: A Review. Sustainability, 14(15), pp. 9120.
[13] ANGEL, N.A., RAVINDRAN, D., P M DURAI, R.V., SRINIVASAN, K. and YUH-CHUNG, H., 2022. Recent Advances in Evolving Computing Paradigms: Cloud, Edge, and Fog Technologies. Sensors, 22(1), pp. 196.
[14] BAYOMI, N. and FERNANDEZ, J.E., 2023. Eyes in the Sky: Drones Applications in the Built Environment under Climate Change Challenges. Drones, 7(10), pp. 637.
[15] BHARATI, S. and PODDER, P., 2022. Machine and Deep Learning for IoT Security and Privacy: Applications, Challenges, and Future Directions. Security and Communication Networks, 2022.
[16] CHATAUT, R., PHOUMMALAYVANE, A. and AKL, R., 2023. Unleashing the Power of IoT: A Comprehensive Review of IoT Applications and Future Prospects in Healthcare, Agriculture, Smart Homes, Smart Cities, and Industry 4.0. Sensors, 23(16), pp. 7194.
[17] DAWOOD, M., TU, S., XIAO, C., ALASMARY, H., WAQAS, M. and REHMAN, S.U., 2023. Cyberattacks and Security of Cloud Computing: A Complete Guideline. Symmetry, 15(11), pp. 1981.
[18] DEMERTZI, V., DEMERTZIS, S. and DEMERTZIS, K., 2023. An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities. Applied Sciences, 13(2), pp. 790.
[19] GEORGE, W. and AL-ANSARI, T., 2023. Review of Blockchain Applications in Food Supply Chains. Blockchains, 1(1), pp. 34.
[20] HAMZAH, M., MD, M.I., HASSAN, S., MD, N.A., MOST, J.F., MUHAMMED, B.J. and ALI, W.M., 2023. Distributed Control of Cyber Physical System on Various Domains: A Critical Review. Systems, 11(4), pp. 208.
[21] HASSANI, H., AVDIU, K., UNGER, S. and MAEDEH, T.M., 2023. Blockchain in the Smart City and Its Financial Sustainability from a Stakeholder's Perspective. Journal of Risk and Financial Management, 16(9), pp. 393.
[22] HASSEBO, A. and TEALAB, M., 2023. Global Models of Smart Cities and Potential IoT Applications: A Review. IoT, 4(3), pp. 366.
[23] KALEEM, S., SOHAIL, A., TARIQ, M.U., BABAR, M. and QURESHI, B., 2023. Ensemble learning for multi-class COVID-19 detection from big data. PLoS One, 18(10),.
[24] KANTSEPOLSKY, B. and AVIV, I., 2024. Sensors in Civil Engineering: From Existing Gaps to Quantum Opportunities. Smart Cities, 7(1), pp. 277.
[25] KHAN, Y., MAZLIHAM BIN MOHD SU'UD, MUHAMMAD, M.A., SAYED, F.A., NUR, A.S. and KHAN, N., 2023. Architectural Threats to Security and Privacy: A Challenge for Internet of Things (IoT) Applications. Electronics, 12(1), pp. 88.
[26] KOUKARAS, P., AFENTOULIS, K.D., GKAIDATZIS, P.A., MYSTAKIDIS, A., IOANNIDIS, D., VAGROPOULOS, S.I. and TJORTJIS, C., 2024. Integrating Blockchain in Smart Grids for Enhanced Demand Response: Challenges, Strategies, and Future Directions. Energies, 17(5), pp. 1007.
[27] KRICHEN, M., 2023. Formal Methods and Validation Techniques for Ensuring Automotive Systems Security. Information, 14(12), pp. 666.
[28] KUMAR, A., SHARMA, S., SINGH, A., ALWADAIN, A., BONG-JUN CHOI, MANUAL-BRENOSA, J., ORTEGA-MANSILLA, A. and GOYAL, N., 2022. Revolutionary Strategies Analysis and Proposed System for Future Infrastructure in Internet of Things. Sustainability, 14(1), pp. 71.
[29] LAKSHMI, V. and CORBETT, J., 2023. Using AI to Improve Sustainable Agricultural Practices: A Literature Review and Research Agenda. Communications of the Association for Information Systems, 53, pp. 96-137.
[30] LI, J., MAITI, A. and FEI, J., 2023. Features and Scope of Regulatory Technologies: Challenges and Opportunities with Industrial Internet of Things. Future Internet, 15(8), pp. 256.