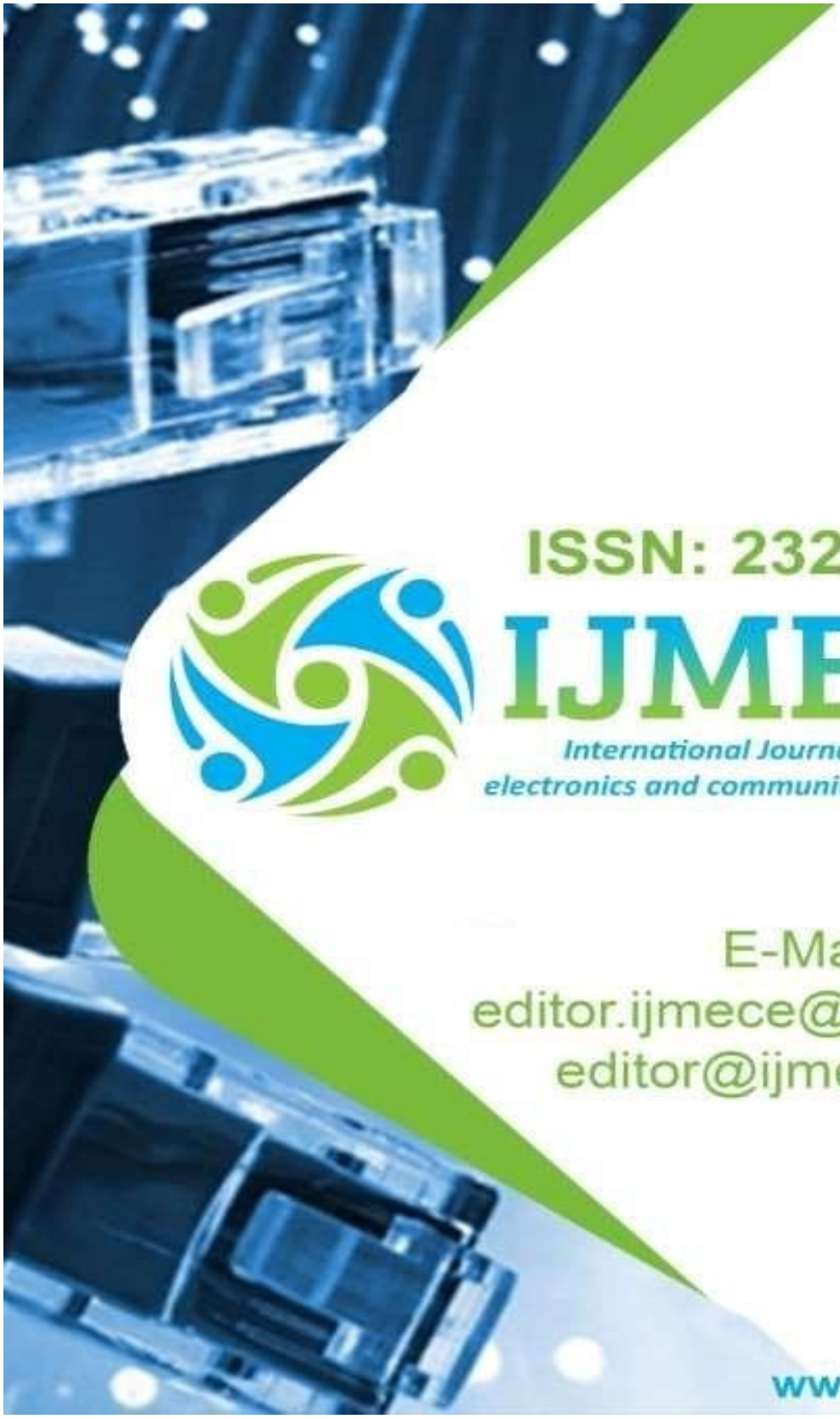

ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

Sharing user IoT Devices in the Cloud

Gurrala Shiva kumari [1], Torlapati Venkateswara Rao [2]
Assistant professor, department of ECE, St. Martin's Engineering college
1Assistant Professor, Department of CSE, Sree Vahini Institute ofScience & Technology (A), Tiruvuru.
Email: vinnuyadav907@gmail.com

Abstract: The Internet of Things (IoT) surrounded a range of technologies that enable the interconnection of various devices, from everyday objects to more advanced networked systems. The IoT model is continuously expanding the number of devices owned by individuals. Similar to the concept of social networks, IoT-based social networks would enable users to share devices, which could provide valuable information captured by sensors or allow remote actions to be performed on user devices. This paper introduces an IoT-focused social device network built on a Cloud computing model, which offers a virtual execution environment due to its decentralized structure, high reliability and accessibility anytime, anywhere. The paper outlines an approach that simplifies the reuse of widely distributed IoT resources by creating services on top of them. These services are then used to build applications, which are deployed on service platforms hosted in the Cloud, ensuring secure access to the data shared by these devices while maintaining compliance.

Keywords: Internet of Things (IoT), Social Networks, Cloud Computing Model, Virtual Execution Environment, social Device Network, Reliability, Accessibility.

I. INTRODUCTION

The Internet of Things (IoT) has emerged as a foundation of modern technological ecosystems, enabling everyday objects to connect, communicate and share data through the internet. As IoT devices increase rapidly across homes, businesses and industries, the demand for scalable and flexible infrastructure to manage these devices has grown exponentially. Cloud computing has provided an ideal solution, offering vast storage, processing power and real-time accessibility. By leveraging cloud technologies, users can store, analyze, and share data from IoT devices, enabling seamless interaction across different platforms and geographies. This convergence of IoT and cloud computing is paving the way for innovative services and applications that rely on the interrelated of devices and data.

Sharing IoT devices in the cloud is a key aspect of this evolution, allowing multiple users or organizations to access and utilize devices remotely without being restricted by geographic or physical limitations. This capability enables shared ownership, cost optimization and greater utilization of resources. For example, a smart thermostat in a shared office space or a network of sensors used for environmental monitoring in multiple locations can be centrally managed and shared via the cloud. This model fosters greater collaboration and resource efficiency while allowing users to benefit from the full potential of IoT technology without the need for excessive upfront investment in infrastructure.

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

The cloud-based sharing of IoT devices also opens the door to new opportunities for data-driven decision-making. As IoT devices collect vast amounts of data, cloud platforms provide the necessary computational power to process, store and analyze this information at scale. Users can access detailed insights in real-time, enabling informed decisions on everything from energy consumption and predictive maintenance to inventory management and environmental monitoring. The cloud-based sharing model facilitates the aggregation of data from multiple sources, unlocking powerful opportunities for analytics and machine learning applications, which can optimize processes and improve efficiency across sectors.

However, the sharing of IoT devices in the cloud introduces several challenges that need to be addressed to ensure a secure, reliable and efficient environment. Security concerns, such as data privacy, unauthorized access, and vulnerabilities in the devices themselves, must be mitigated through robust encryption, authentication and access control mechanisms. Furthermore, ensuring data integrity, handling device interoperability, and managing the complexities of different cloud environments are critical to the success of such systems. Addressing these issues will be vital to realizing the full potential of IoT device sharing in the cloud while maintaining the trust and confidence of users.

With the rise of personal computers and smart phones, the IoT pattern has significantly increased the number of devices owned by individuals. These devices have become an integral part of daily life, aimed at enhancing the overall quality of living. They come in various forms, including sensor devices that monitor environmental factors such as humidity, temperature, motion, pollution and noise levels, as well as those that track user related information such as location, health and emotions. Additionally, actuator devices, such as light switches, displays, and motorized shutters, are designed to perform actions that alter the state of physical environments (like a room, building, or city) or virtual systems [1].

II. LITERATURE SURVEY

M. Kumar and R. B. Agnihotri et al. Internet of Things (IOT) is the way to dealing with technology to get the inter connection with any devices which is ubiquitous in nature as well as for the new generation devices which ultimately bring the various daily usage devices to make it more complex and integrated with network devices. The IOT socially provided network could allow the sharing of devices among the users which could combined provide the useful information which the sensors will capture through which the remote actions could be established. This research provides the cloud-based technology to embed to work regarding the IOT centred social device which provides the virtualized environment for any execution of further processes and being graceful to its non-centralized behaviour, highly reliable and accessible from anywhere and even at any time. It basically deals with the reusability of IOT resources by getting to action as a service,

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

where the applications are made by the combination of various services which is deployed in a platform which could be hosts in cloud-platform which allows the secured accessibility of services as well as the data by the combining and compiling these IOT devices [2].

N. Kitagawa, A. Takefusa and K. Aida et al. Research on Internet of Things (IoT) application systems, which store data collected by various sensor devices to a cloud and utilize the data through statistical analysis and machine learning, has been conducted extensively. Several platforms have been proposed to support the development of IoT application systems, which enable system administrators to easily manage edge hardware and group sensors. However, conventional development support platforms do not provide functions for secure data management, such as encryption processing when handling confidential information and flexible access control among members of a research group. In this paper, we propose a mechanism for securely and easily encrypting data and sharing data using a Secure Configuration Server. We have been developing "SINETStream," an IoT application development support tool provided by National Institute of Informatics, Japan. The secure configuration server can co-work with the SINETStream-based IoT systems. This mechanism enables easy sharing of confidential information by securely managing data encryption keys within the system, which has been complicated with conventional methods. In addition, our mechanism provides users with confidential information in an encrypted form, so that only authorized users can view the data [3].

S. Katta, K. Alrawashdeh, J. Adebayo, M. Tulasi and M. Dokka et al. The growing usage of Internet of Things (IoT) devices has led to a need for secure and decentralized identity management systems. Scalability and security are two major problems with traditional centralized identity management systems. In this paper, we propose a distributed hybrid cloud identity management system based on the blockchain for protecting IoT devices in the cloud. To achieve scalability, reliability, and performance, our system makes use of the advantages of distributed architecture and blends the characteristics of public and private cloud infrastructures. Blockchain technology is used for generating an auditable and tamper-proof record of identity management transactions. Our technology offers a decentralized and reliable identity management system, ensuring the privacy and security of IoT devices. Our proposed system provides a promising solution for managing the identities of IoT devices in a secure and decentralized manner, thus mitigating the security risks associated with centralized identity [4].

M. Y. Idris, D. Stiawan, N. M. Habibullah, A. H. Fikri, M. R. Abd Rahim and M. Dasuki et al. Centralized e-Learning technology has dominated the learning ecosystem that brings a lot of potential usage on media rich learning materials. However, the centralized architecture has their own constraint to support large number of users for accessing large size of learning

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

contents. On the other hand, Content Delivery Network (CDN) solution which relies on distributed architecture provides an alternative solution to eliminate bottleneck access. Although CDN is an effective solution, the implementation of technology is expensive and has less impact for student who lives in limited or non-existence internet access in geographical area. In this paper, we introduce an IoT smart device to provide e-Learning access for content sharing on hybrid cloud environment with distributed peer-to-peer communication solution for data synchronization and updates. The IoT smart device acts as an intermediate device between user and cloud services, and provides content sharing solution without fully depending on the cloud server [5].

T. Primya, S. M, V. Ramya, S. R. Taanusri, G. Ridhanya and R. A. Sekar et al. Smart gadgets can now communicate from close to a long distance with one another and with the Internet or cloud. Internet of things (IOT) brings a paradigm shift of employing low resource IOT smart system with cloud computing. However, by employing cloud computing, resource-constrained IoT smart devices can gain a number of advantages, Excluding the weight of data processing and storing the data on the network cloud. By implementing it on network edge offers more merits instead of using network cloud in contra to internet of things (IOT) applications which needs high data rates, mobility, and latency-sensitive real-time data processing. In this paper mainly focused on data transfers to cloud and IOT devices form smart data transfer. Here a suggestion that is authenticated search method to look for required information among one's personal or shared data on storage. At last, by evaluating processing time performance of the suggested scheme, outcomes that discussed in the paper, show that our strategy has a chance of working well in IoT applications [6].

III. METHODOLOGY

The sharing user IoT devices in the cloud involves several key steps, starting with device registration and cloud integration. The first stage focuses on enabling IoT devices to connect to a cloud platform. This requires each device to be equipped with appropriate communication protocols (such as Wi-Fi, Bluetooth, or cellular networks) and an embedded agent capable of interacting with the cloud. Through APIs and SDKs, these devices transmit data to cloud servers for storage, processing and remote access. Users are then required to register their devices on the cloud platform, providing necessary metadata such as device type, location, and functionalities. Once registered, the devices become accessible for sharing with other users or systems.

Next, the cloud platform needs to facilitate user access and device management. The platform typically employs a web camera or laptop interface, where users can control and configure devices remotely. This interface also includes user authentication and authorization mechanisms, ensuring that only authorized individuals or systems can access and interact with the devices. Cloud platforms generally use Role Based Access Control (RBAC) or other access management techniques to grant permissions, ensuring that users can only

perform actions according to their designated roles. Furthermore, to enable sharing among multiple users, the platform supports the creation of user groups or shared device pools, allowing users to collaborate and utilize devices collectively.

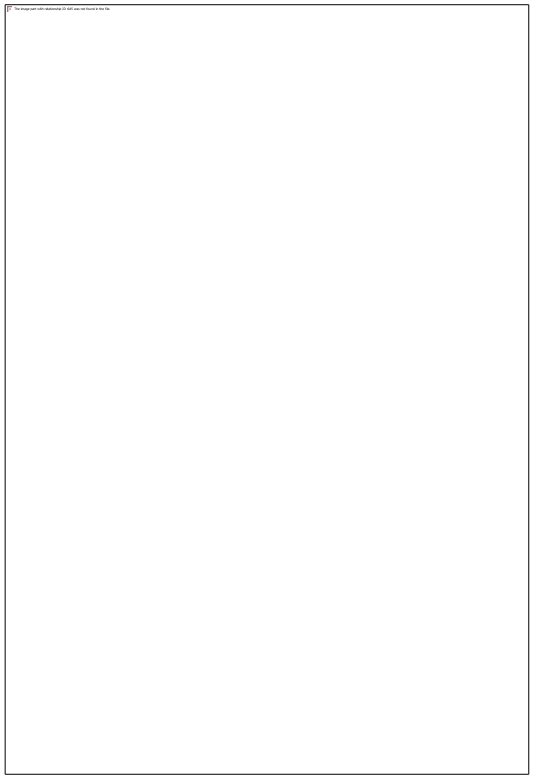

Fig. 1: Block Diagram

To ensure interoperability between different types of IoT devices, the cloud platform must implement device abstraction and standardization. Given the diversity of IoT devices, ranging from sensors to actuators, it is crucial that the platform can manage various protocols and data formats. Middleware or cloud-based software frameworks are often employed to bridge these differences, providing a unified interface for users and enabling seamless communication between devices. This abstraction layer also helps in adapting to future device integrations, as new devices and technologies can be added without disrupting the existing system.

Data management is another critical aspect of the methodology. As IoT devices generate vast amounts of data, efficient storage, processing, and retrieval mechanisms are essential. Cloud platforms typically store data in scalable databases or distributed storage systems to handle large volumes. For real-time use cases, edge computing may be implemented, where data is processed locally on the edge devices before being sent to the cloud. This reduces latency and bandwidth consumption. Furthermore, the cloud platform analyzes the data using machine learning models or analytics tools to provide actionable insights to users. Data privacy and security measures are integrated into this process, ensuring that sensitive information, such as health data or location details, is protected from unauthorized access.

A proxy to the cloud acts as an intermediary layer between IoT devices and cloud platforms, facilitating communication and data transfer. It helps manage device connectivity, ensuring secure and efficient transmission of data to the cloud by handling tasks like data aggregation, filtering, and encryption. The proxy can also enable devices with limited capabilities to interact with cloud services by translating communication protocols or protocols mismatches. This intermediary layer ensures that IoT devices can securely connect to the cloud without direct exposure to external networks, improving scalability, security, and data integrity in IoT ecosystems.

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

Finally, the sharing of IoT devices in the cloud must be managed to ensure reliability, scalability, and security. The cloud infrastructure must support multiple users accessing and controlling devices simultaneously, without performance degradation. Load balancing and distributed computing are essential to accommodate high traffic and ensure smooth operations. In terms of security, encryption protocols, secure communication channels, and multi-factor authentication are implemented to safeguard data transmission and device access. Moreover, regular updates and monitoring are necessary to ensure that devices are functioning optimally and to detect any potential vulnerabilities. By integrating these practices, the sharing of IoT devices in the cloud can operate efficiently and securely, providing users with a reliable, flexible, and scalable solution.

IV. RESULTS

In this section performance analysis of sharing user IoT Devices in the Cloud is observed.

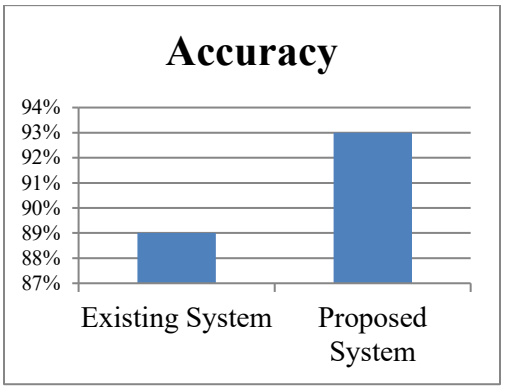

Fig. 2: Accuracy Comparison Graph

In figure 2 shows the accuracy comparison graph is observed between existing system and proposed system. The proposed system shows the high accuracy.

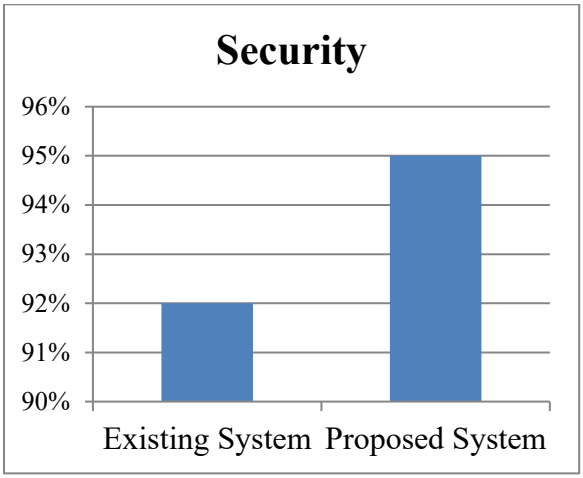

Fig. 3: Security Comparison Graph

In figure 3 shows the security comparison graph is observed between existing system and proposed system. The proposed system shows the high security.

V. CONCLUSION

The integration of IoT with cloud computing presents a powerful framework for building a social device network that enhances the sharing and utilization of IoT resources. By leveraging the decentralized, reliable and accessible nature of the cloud, this model enables users to access and control devices remotely while ensuring data security and accuracy. The approach outlined in this paper demonstrates how distributed IoT resources can be efficiently repurposed through service-oriented architectures, facilitating the development of diverse applications. This innovation fosters greater collaboration, resource optimization, and the creation of smart, interconnected environments, the way for more flexible and scalable IoT solutions in the future.

VI. REFERENCES

[1] Y. Benazzouz, C. Munilla, O. Günalp, M. Gallissot and L. Gürgen, "Sharing user IoT devices in the cloud," 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea (South), 2014, pp. 373-374, doi: 10.1109/WF-IoT.2014.6803193.

[2] M. Kumar and R. B. Agnihotri, "Sharing Unused User IoT Devices in the Cloud," 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2019, pp. 400-403, doi: 10.1109/ICECA. 2019.8822118.

[3] N. Kitagawa, A. Takefusa and K. Aida, "Development of a Secure Data Sharing Mechanism for IoT Application Systems," 2022 IEEE 11th International Conference on Cloud Networking (CloudNet), Paris, France, 2022, pp. 131-135, doi: 10.1109/CloudNet55617.2022.9978835.

[4] S. Katta, K. Alrawashdeh, J. Adebayo, M. Tulasi and M. Dokka, "Blockchain-Based Distributed Hybrid Cloud Identity Management for Securing IoT Devices in the Cloud," NAECON 2023 - IEEE National Aerospace and Electronics Conference, Dayton, OH, USA, 2023, pp. 67-72, doi: 10.1109/NAECON58068.2023.10365929.

[5] M. Y. Idris, D. Stiawan, N. M. Habibullah, A. H. Fikri, M. R. Abd Rahim and M. Dasuki, "IoT smart device for e-leaming content sharing on hybrid cloud environment," 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Yogyakarta, Indonesia, 2017, pp. 1-5, doi: 10.1109/EECSI.2017.8239078.

[6] T. Primya, S. M, V. Ramya, S. R. Taanusri, G. Ridhanya and R. A. Sekar, "Data sharing in Cloud-Assisted IoT," 2023 Eighth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Chennai, India, 2023, pp. 1-8, doi: 10.1109/ICONSTEM56934.2023. 10142285.

[7] M. Azam and E. N. Huh, "Inter-cloud media storage and media cloud architecture for inter-cloud communication", 2014 IEEE 7th International Conference on Cloud Computing, pp. 982-985, 2014, June.

[8] M. Joshi, K. Joshi and T. Finin, "Attribute Based Encryption for Secure Access to Cloud Based EHR Systems"in , UMBC Information Systems Department Collection, 2018.

[9] T. Shah and S. Venkatesan, "Authentication of IoT Device and IoT Server Using Secure Vaults", 2018 17th IEEE International Conference on Trust Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 819-824, 2018, August.

[10] A. R. Biswas and R. Giaffreda, "IoT and cloud convergence: Opportunities and challenges", 2014 IEEE World Forum on Internet of Things (WF-IoT), pp. 375-376, 2014, March.

[11] S. G. Hong, N. S. Kim and T. Heo, "A smartphone connected software updating framework for IoT devices", 2015

International Symposium on Consumer Electronics (ISCE), pp. 1-2, 2015, June.

[12] P. K. Gupta, V. Tyagi and S. K. Singh, "Applications of Predictive Computing" in Predictive Computing and Information Security, Singapore:Springer, pp. 137-155, 2017.

[13] P. Diogo, L. P. Reis and N. V. Lopes, "Internet of Things: A system's architecture proposal", 2014 9th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1-6, 2014, June.

[14] S. Sundareswaran, A. Squicciarini and D. Lin, "A brokerage-based approach for cloud service selection", 2012 IEEE Fifth International Conference on Cloud Computing, pp. 558-565, 2012, June.

[15] P. Xiong, Y. Chi, S. Zhu, H. J. Moon, C. Pu and H. Hacigümüs, "Intelligent management of virtualized resources for database systems in cloud environment", 2011 IEEE 27th International Conference on Data Engineering, pp. 87-98, 2011, April.

[16] C. Ward, N. Aravamudan, K. Bhattacharya, K. Cheng, R. Filepp, R. Kearney, et al., "Workload migration into clouds challenges experiences opportunities", 2010 IEEE 3rd International Conference on Cloud Computing, pp. 164-171, 2010, July.

[17] A. Passarella, "A survey on content-centric technologies for the current Internet: CDN and P2P solutions", Computer Communications, vol. 35, pp. 1-32, 2012.

[18] S. Shapsough, M. Hassan, S. E. Shapsough and I. A. Zualkernan, "IoT Technologies to Enhance Precision and Response Time of Mobile-Based Educational Assessments", 2016 International Conference on Computational Science and Computational Intelligence (CSCI), pp. 202-205, 2016.

[19] D. Stiawan, M. Y. Idris, R. F. Malik, S. Nurmaini and R. Budiarto, "Anomaly detection and monitoring in Internet of Things communication", 2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE), pp. 1-4, 2016.

[20] T. M. C. Simões, J. J. P. C. Rodrigues, J. E. F. Costa and M. L. Proença, "E-learning solutions for cloud environments", 2012 IEEE Latin America Conference on Cloud Computing and Communications (LatinCloud), pp. 55-59, 2012.