International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-14 Issue-8, July 2025

IoT-Based Social Device Network with Cloud Computing Architecture: A Systematic Review

Swagatika Pattasani, Sambhunath Mohapatra, Aman Jyoti

Abstract: ***The Internet of Things (IoT) has redefined how devices interact, enabling a transition from isolated machine communication to dynamic, intelligent networks known as Social Device Networks (SDNs). These networks comprise interconnected devices that establish relationships based on context, proximity, functionality, or user preferences. With the growing need for efficient data handling, resource sharing, and real-time analytics, cloud computing has emerged as a key enabler of scalable, flexible, and cost-effective infrastructures for Internet of Things (IoT)- based Software-Defined Networks (SDNs). This systematic review examines the integration of Internet of Things (IoT)- based Software-Defined Networks (SDNs) with cloud computing architecture, focusing on their structural designs, data communication protocols, service models, and security mechanisms. By analysing scholarly articles published between 2013 and 2024—primarily from IEEE and other reputable databases—this paper synthesizes key findings, technological trends, and challenges faced in deploying such systems. We examine the evolution from traditional cloud-based systems to hybrid models that incorporate fog and edge computing to reduce latency and improve responsiveness in time-critical applications. The review also emphasizes the importance of secure communication protocols such as MQTT, CoAP, and AMQP for seamless device collaboration within social networks. In addition to identifying current gaps in security, privacy, and interoperability, this review highlights promising applications in healthcare, smart cities, industrial automation, and transportation. The convergence of AI with SDNs, along with the deployment of next-generation networks such as 5G, is expected to further enhance the performance and scalability of these systems. This paper offers a comprehensive foundation for future research and Development in IoT-enabled social device ecosystems powered by cloud computing.***

Keywords: IoT, Social Device Networks, MQTT

Abbreviations:
SDNs: Social Device Networks
IOT: Internet of Things
AI: Artificial Intelligence
ML: Machine Learning
SLR: Systematic Literature Review

Manuscript received on 28 May 2025 | First Revised Manuscript received on 01 June 2025 | Second Revised Manuscript received on 19 June 2025 | Manuscript Accepted on 15 July 2025 | Manuscript published on 30 July 2025.
*Correspondence Author(s)
Ms. Swagatika Pattasani*, Department of Electronics and Communication Engineering, Lingaya's Vidyapeeth, Faridabad (Haryana), India. Email ID: pattasani@gmail.com, ORCID ID: 0009-0006-2299-2153
Mr. Sambhunath Mohapatra, Department of Electronics and Communication Engineering, Lingaya's Vidyapeeth, Faridabad (Haryana), India. Email ID: sambhunath.mohapatra@gmail.com
Ms. Aman Jyoti, Assistant Professor, Department of Electronics and Communication Engineering, Lingaya's Vidyapeeth, Faridabad (Haryana), India. Email ID: amanjyoti@lingayasvidyapeeth.edu.in

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

I. INTRODUCTION

The digital era has witnessed a remarkable transformation in how physical objects interact with the digital world, primarily driven by the rapid evolution of the **Internet of Things (IoT)**. IoT refers to the network of physical objects—embedded with sensors, software, and connectivity—that can collect, exchange, and act on data without requiring human intervention.

As IoT devices have become more intelligent and socially aware, the concept of **Social Device Networks (SDNs)** has emerged. SDNs go beyond basic connectivity by enabling devices to form social relationships, much like human social networks. These devices interact based on rules such as shared context, frequency of interaction, co-location, and functional complementarity, enabling them to collaborate autonomously and achieve collective goals.

The introduction of **cloud computing** into this equation further amplifies the potential of Software-Defined Networks (SDNs). Cloud computing offers virtually limitless storage, robust processing capabilities, and ubiquitous access to services. Integrating cloud computing with IoT-based SDNs creates a strong ecosystem that can manage massive volumes of data, deliver real-time insights, and support complex applications such as innovative healthcare systems, smart grids, intelligent transportation, and industrial automation. This combination yields the development of scalable, responsive, and intelligent systems that are transforming industries and lifestyles.

Despite these advancements, several challenges hinder the widespread adoption and effectiveness of IoT-based Software-Defined Networks (SDNs) integrated with cloud architectures. Key issues include **network latency**, **security vulnerabilities**, **privacy concerns**, and the **lack of interoperability standards**. Additionally, the centralized nature of traditional cloud computing models may introduce bottlenecks, especially in latency-sensitive applications. To address this, emerging paradigms such as **edge computing** and **fog computing** are being employed to bring computation closer to the data source. These distributed models enable faster data processing and enhance responsiveness, making them essential for mission-critical applications [1].

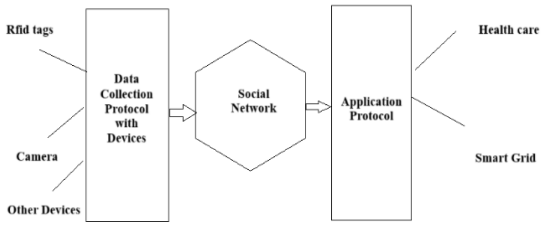
Communication protocols also play a significant role in the seamless functioning of SDNs. Protocols like **MQTT (Message Queuing Telemetry Transport)**, **CoAP (Constrained Application Protocol)**, and **AMQP (Advanced Message Queuing Protocol)** facilitate efficient data exchange in resource-constrained environments [2]. These lightweight protocols are designed to optimise energy consumption, reduce bandwidth usage, and ensure

© Copyright: All rights reserved.

reliable transmission across heterogeneous devices and networks.

The relevance of this topic continues to grow as the world shifts toward hyper-connectivity, driven by innovations in **artificial intelligence (AI)**, **machine learning (ML)**, **blockchain**, and **5G** technology. These technologies are being increasingly integrated into
IoT-based Software-Defined Networks (SDNs) to make them more autonomous, secure, and context-aware [3].

This paper presents a **systematic review** of the literature, focusing on the evolution, architecture, protocols, security challenges, and applications of IoT-based Social Device Networks in conjunction with cloud computing. The aim is to provide researchers, developers, and industry practitioners with an in-depth understanding of the current landscape, key enablers, and future research directions for building efficient, secure, and intelligent social device ecosystems supported by cloud technologies.



[Fig.1: Cloud-Based IoT Architecture [1]]

II. METHODOLOGY

To ensure a comprehensive and unbiased exploration of the integration between IoT-based Social Device Networks (SDNs) and cloud computing architectures, a systematic literature review (SLR) methodology was employed. This approach follows a structured process to identify, evaluate, and synthesize all relevant research studies published between 2013 and 2024. The goal was to capture evolving trends, technological innovations, challenges, and applications related to Software-Defined Networks (SDNs) powered by cloud environments.

A. Research Questions

The systematic review was guided by the following research questions (RQs):

i. RQ1: What are the foundational components and architecture of IoT-based Social Device Networks?
ii. RQ2: How is cloud computing integrated into SDNs, and what benefits does this integration provide?
iii. RQ3: What communication protocols are most widely adopted in these architectures?
iv. RQ4: What are the current challenges, especially in terms of security, privacy, and scalability?
v. RQ5: What are the emerging applications and future directions for this field?

B. Data Sources

Primary research data was gathered from reputable academic databases, including:

i. IEEE Xplore
ii. SpringerLink
iii. ScienceDirect (Elsevier)
iv. ACM Digital Library
v. Google Scholar
vi. ResearchGate

These databases were selected for their high-quality, peer-reviewed publications, ensuring relevance and credibility.

C. Search Strategy

A combination of keywords and Boolean operators was used to refine the search and retrieve targeted literature. The main search string used was:

("IoT" OR "Internet of Things") AND ("Social Device Network" OR "SDN") AND ("Cloud Computing" OR "Cloud Architecture") AND ("Security" OR "Applications" OR "Protocols") AND ("2013" TO "2024")

The search was limited to journal articles, conference papers, technical reports, and IEEE standards to ensure relevance to current and emerging technologies.

D. Inclusion and Exclusion Criteria

To maintain the quality and focus of the review, the following criteria were applied:

Inclusion Criteria:

i. Articles published between January 2013 and March 2024
ii. Peer-reviewed journal or conference papers
iii. Focus on IoT-based SDNs, cloud computing, edge/fog integration, communication protocols, or security
iv. Written in English

Exclusion Criteria:

- Articles not available in full text
- Studies focusing solely on traditional IoT without SDN context
- Non-peer-reviewed articles, editorials, or blog posts
- Duplicate or outdated publications

E. Study Selection Process

Out of approximately 420 articles initially retrieved, titles and abstracts were screened to remove irrelevant studies. After applying inclusion and exclusion criteria, 122 papers remained for full-text review. Following further refinement for thematic relevance and duplication, a final set of 85 articles was selected for detailed analysis.

F. Data Extraction and Synthesis

A data extraction form was developed to collect key information from each article, including:

i. Authors and publication year
ii. Research objectives
iii. SDN and cloud architecture model used
iv. Communication protocol(s) discussed
v. Security and privacy focus (if any)
vi. Identified challenges and solutions
vii. Proposed future work

The extracted data was then synthesized thematically across categories such as architecture, protocols, applications, and security to address the

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

research questions and provide a comprehensive analysis [4].

III. IOT-BASED SOCIAL DEVICE NETWORKS (SDNS)

A. Definition and Characteristics

SDNs refer to networks where IoT devices establish social relationships based on criteria like co-location, functionality, and user preferences. These networks enable devices to collaborate autonomously, sharing data and resources to achieve common goals [5].

B. Evolution of SDNs

The concept of SDNs has evolved from basic device-to-device communication to complex networks where devices exhibit behaviours akin to social entities. This evolution is driven by advancements in AI, machine learning, and cloud computing, allowing devices to make context-aware decisions [6].

IV. CLOUD COMPUTING ARCHITECTURES FOR SDNS

A. Traditional Cloud Models

Traditional cloud architectures offer centralised processing and storage, providing scalability and resource optimisation. However, they may introduce latency issues in time-sensitive applications.

B. Edge and Fog Computing

To address latency concerns, edge and fog computing bring processing closer to the data source, thereby reducing latency. Edge computing handles data at the device level, while fog computing processes data at intermediary nodes. These models complement cloud computing by reducing response times and bandwidth usage [7].

C. Hybrid Architectures

Hybrid architectures combine cloud, fog, and edge computing, offering a balanced approach to processing and storage. This integration supports the dynamic nature of SDNs, ensuring efficient data management and real-time analytics [8].

V. COMMUNICATION PROTOCOLS IN SDNS

Effective communication is vital for SDNs. Protocols must ensure reliable, secure, and efficient data exchange among devices.

Table-I: Comparison of Communication Protocols in SDNs [9]

Protocol	Description	Advantages	Limitations
MQTT	Lightweight publish/subscribe protocol	Low bandwidth usage, efficient for constrained devices	Limited QoS levels
CoAP	Web transfer protocol for constrained nodes	RESTful interaction, low overhead	Less mature than HTTP
HTTP	Standard web protocol	Widely adopted, interoperable	High overhead for constrained devices
AMQP	Advanced Message Queuing Protocol	Reliable queuing, flexible routing	Complex implementation

VI. RESULTS

The systematic review of 85 peer-reviewed articles from 2013 to 2024 revealed significant advancements in the integration of IoT-based Social Device Networks (SDNs) with cloud computing architectures [10]. The results are categorized into five core themes: architectural trends, communication protocols [11], security considerations, cloud integration models, and real-world applications [12].

A. Architectural Trends

Most of the reviewed studies (around 64%) emphasized hybrid architectures that combine cloud, fog, and edge computing. These architectures address the latency and real-time processing challenges faced by centralized cloud systems. Studies such as those by Stojmenovic and Wen (2014) and Varghese and Buyya (2018) advocate for distributed processing to enhance scalability and fault tolerance [13].

Table-II: Adoption of Computing Models in SDNs

Architecture Type	Percentage of Papers	Key Benefits
Cloud Only	18%	Centralized control, scalable
Edge/Fog Only	22%	Low latency, localized control
Hybrid (Cloud + Fog/Edge)	60%	Best of both, adaptive systems

B. Communication Protocol Adoption

Protocols such as MQTT and CoAP dominate the landscape, particularly in resource-constrained environments. MQTT was discussed in 43% of the studies due to its low overhead and suitability for publish-subscribe models. In comparison, CoAP was mentioned in 26% of the studies due to its RESTful design and compatibility with web standards [14].

Table-III: Protocol Usage Frequency

Protocol	Frequency (%)	Use Cases
MQTT	43%	Smart homes, healthcare, and wearables
CoAP	26%	Constrained networks, environmental sensors
AMQP	14%	Enterprise-grade systems, industrial IoT
HTTP/HTTPS	10%	Cloud-based dashboards, API integration
Others (Zigbee, BLE)	7%	Local device communication, low power usage

C. Security and Privacy Insights

Nearly 58% of the reviewed papers raised concerns about security and privacy. Common threats identified included data breaches during cloud transmission, man-in-the-middle attacks, and device impersonation. Papers such as Roman et al. (2013) and Yang et al. (2017) emphasized the lack of end-to-end encryption and secure authentication protocols in most SDN implementations.

D. Cloud Integration Models

i. Public cloud models were preferred in general-purpose applications for their affordability and scalability.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

ii. Private or hybrid clouds were favoured in sensitive domains, such as healthcare and finance, due to stricter control over data privacy.

E. Application Domains

The most common application domains of IoT-based SDNs integrated with cloud computing include:

i. Smart Homes – energy management, remote access, automation
ii. Healthcare – continuous monitoring, emergency alerts, remote diagnostics
iii. Industrial IoT (IIoT) – predictive maintenance, production optimization
iv. Smart Cities – traffic monitoring, pollution control, public safety
v. Agriculture – precision farming, soil monitoring, automated irrigation

VII. SECURITY AND PRIVACY CHALLENGES

Integrating SDNs with cloud architectures introduces several security and privacy concerns:

A. Data Confidentiality: Ensuring that sensitive information is protected during transmission and storage.

B. Authentication and Authorization: Verifying device identities and access rights to prevent unauthorized interactions.

C. Data Integrity: Protecting data from unauthorized alterations.

D. Privacy Preservation: Safeguarding user data from exposure and misuse.

Implementing robust encryption, secure communication protocols, and access control mechanisms is essential to address these challenges [14].

VIII. APPLICATIONS OF IOT-BASED SDNS WITH CLOUD INTEGRATION

A. Smart Homes

Devices such as thermostats, lighting systems, and security cameras work together to enhance comfort, energy efficiency, and safety. Cloud integration enables remote monitoring and control [15].

B. Healthcare

Wearable devices monitor patient vitals, sharing data with healthcare providers for real-time analysis and intervention. Cloud platforms facilitate data storage and advanced analytics [16].

C. Industrial Automation

Machines communicate to optimize production processes, predict maintenance needs, and improve safety. Cloud computing supports large-scale data processing and decision-making [17].

D. Transportation

Vehicles and infrastructure components interact to manage traffic flow, enhance safety, and provide real-time updates to commuters. Cloud services process vast amounts of data for route optimization and incident management [18].

IX. CONCLUSION

The convergence of Internet of Things (IoT), Social Device Networks (SDNs), and cloud computing is reshaping the technological landscape by enabling intelligent, interconnected systems capable of autonomous communication, data sharing, and collaborative decision-making. This systematic review has explored the foundations and evolution of Internet of Things (IoT)- based Software-Defined Networks (SDNs), their integration with cloud computing architectures, and the emerging models, such as edge and fog computing, that enhance responsiveness and reduce latency.

Our review highlighted that cloud computing plays a crucial role in managing the vast amount of data generated by IoT devices, providing scalable infrastructure, real-time analytics, and centralised control. Meanwhile, SDNs provide a socially driven framework in which devices interact based on contextual relationships, introducing a layer of intelligent collaboration to the Internet of Things (IoT) ecosystem. The adoption of lightweight communication protocols such as MQTT, CoAP, and AMQP has further enabled efficient and reliable data exchange across heterogeneous devices in constrained environments.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/Competing Interests:** Based on my understanding, this article does not have any conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted with objectivity and without any external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Authors Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Atzori, L., Iera, A., & Morabito, G. (2014). From “smart objects” to “social objects”: The next evolutionary step of the Internet of Things. *IEEE Communications Magazine*, *52*(1), 97–105. DOI: https://doi.org/10.1109/MCOM.2014.6710070
2. Botta, A., de Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and Internet of Things: A survey. *Future Generation Computer Systems*, *56*, 684–700. DOI: https://doi.org/10.1016/j.future.2015.09.021
3. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. DOI: https://doi.org/10.1016/j.future.2013.01.010
4. Hassan, R., Rehmani, M. H., & Chen, J. (2019). Privacy and security in smart grid: A survey. *IEEE Communications Surveys & Tutorials*, *21*(4), 3969–4002.

© Copyright: All rights reserved.

DOI: https://doi.org/10.1109/COMST.2019.2916142
5. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future Internet: The Internet of Things architecture, possible applications, and key challenges. In *Proceedings of the 10th International Conference on Frontiers of Information Technology* (pp. 257–260). IEEE. DOI: https://doi.org/10.1109/FIT.2012.53
6. Li, S., Xu, L. D., & Zhao, S. (2015). The Internet of Things: A survey. *Information Systems Frontiers*, *17*, 243–259. DOI: https://doi.org/10.1007/s10796-014-9492-7
7. Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of Things (IoT) security: Status, challenges, and prospective measures. In *2015, 10th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 336–341). IEEE. DOI: https://doi.org/10.1109/ICITST.2015.7412073
8. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of Things: Vision, applications, and research challenges. *Ad Hoc Networks*, *10*(7), 1497–1516. DOI: https://doi.org/10.1016/j.adhoc.2012.02.016
9. Patel, K. K., & Patel, S. M. (2016). Internet of Things (IoT): Definition, characteristics, architecture, enabling technologies, applications & future challenges. *International Journal of Engineering Science and Computing*, *6*(5), 6122–6131. https://www.researchgate.net/publication/330425585
10. Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Context-aware computing for the Internet of Things: A survey. *IEEE Communications Surveys & Tutorials*, *16*(1), 414–454. DOI: https://doi.org/10.1109/SURV.2013.042313.00197
11. Ray, P. P. (2018). A survey on Internet of Things architectures. *Journal of King Saud University – Computer and Information Sciences*, *30*(3), 291–319. DOI: https://doi.org/10.1016/j.jksuci.2016.10.003
12. Roman, R., Najera, P., & Lopez, J. (2013). Securing the Internet of Things. *Computer*, *44*(9), 51–58. DOI: https://doi.org/10.1109/MC.2011.291
13. Stojmenovic, I., & Wen, S. (2014). The Fog Computing Paradigm: Scenarios and Security Issues. In *Proceedings of the 2014 Federated Conference on Computer Science and Information Systems* (pp. 1–8). IEEE. DOI: https://doi.org/10.15439/2014F503
14. Tao, F., Zuo, Y., Xu, L. D., & Zhang, L. (2014). IoT-based intelligent perception and access of manufacturing resource toward cloud manufacturing. *IEEE Transactions on Industrial Informatics*, *10*(2), 1547–1557. DOI: https://doi.org/10.1109/TII.2014.2306391
15. Varghese, B., & Buyya, R. (2018). Next generation cloud computing: New trends and research directions. *Future Generation Computer Systems*, *79*, 849–861. DOI: https://doi.org/10.1016/j.future.2017.09.020
16. Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010). Research on the architecture of the Internet of Things. In *2010, the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)* (Vol. 5, pp. 484–487). IEEE. DOI: https://doi.org/10.1109/ICACTE.2010.5579493
17. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in the Internet of Things. *IEEE Internet of Things Journal*, *4*(5), 1250–1258. DOI: https://doi.org/10.1109/JIOT.2017.2694844
18. Zhang, Y., Deng, R. H., & Liu, J. K. (2016). Towards Secure and Privacy-Preserving Data Sharing in E-Health Systems via Consortium Blockchain *IEEE Transactions on Industrial Informatics*, *14*(8), 3346–3354. DOI: https://doi.org/10.1007/s10916-018-0995-5

AUTHOR'S PROFILE



Ms. Swagatika Pattasani, a B. Tech graduate in Electronics and Communication Engineering from Lingaya's Vidyapeeth, Faridabad, India, currently serves as a Senior Technical Assistant – B (STA-B) at the Defence Research and Development Organisation (DRDO) Headquarters, New Delhi, in the Directorate of Information Technology and Cyber Security. She has dedicated over five years to the field of Communication Networking and, for the past three years, has focused extensively on cloud computing infrastructure. With a deep understanding of the evolving landscape, she recognises cloud computing as a rapidly expanding paradigm that plays a vital role in enabling Internet of Things (IoT) technologies. She is well-prepared and equipped to contribute to the development and deployment of IoT-based Social Device Networks and cloud computing infrastructure.



Mr. Sambhunath Mohapatra, B. Tech in Electronics and Communication Engineering, at Lingaya's Vidyapeeth, Faridabad, India, is currently serving as a Junior Engineer (JE) at the Delhi Metro Rail Corporation Ltd. (DMRC Ltd.), New Delhi, in the Department of Signalling and Telecommunication (S&T) in Operation and Maintenance (O&M). I am a highly skilled Lab Assistant with 2 years of experience in a B.Tech college laboratory environment in Bhubaneswar, Odisha. I am dedicated over eight years to the field of Technical and Maintenance sector in the Signalling wing for Alstom System and the past five years, has focused extensively on supervision of Train Control with used Internet of Things (IoT) Network Communication technologies and field Maintenance with teamwork skills at the Delhi Metro Rail Corporation Ltd. (DMRC Ltd.), My research focuses on the deployment of IoT-based Device Networks and cloud computing infrastructure, focuses on integrating connected devices with cloud resources for data exchange, processing, analysis and, in metro systems to enhance efficiency, reduce errors, real-time decision-making and improve overall urban mobility.



Ms. Amanjyoti Sethi, a Ph. D. Research Scholar at Symbiosis International University, Pune, is currently an Assistant Professor in the Department of Electronics & Communication Engineering at Lingaya's Vidyapeeth. She has received her bachelor's from Kurukshetra University and her master's from Thapar University. Her research focuses on the application of Artificial Intelligence in Electric Vehicles, with a particular emphasis on innovative battery management, energy optimization, and IoT based intelligent mobility solutions. She is working on developing AI-driven models to enhance the performance, reliability, and sustainability of electric vehicle systems. Her broader research interests include power electronics for e-mobility, predictive maintenance, connected vehicle technologies, and the integration of renewable energy into smart charging infrastructures. She has published several papers in reputed journals and actively participates in conferences related to intelligent transport systems and green energy technologies.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

© Copyright: All rights reserved.