JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
ICASET
2024

Research Article
Collection: Intelligent Computing of Applied Sciences and Emerging Trends

Unveiling the Security Maze: A Comprehensive Review of Challenges in Internet of Things

M. Imran Khan Khalil[1*], Izaz Ahmad Khan[2], Asif Nawaz[3], Shahid Latif[4], Sheeraz Ahmad[4], and Safyan Ahmed[5]

[1]University of Engineering & Technology, Peshawar, 25000, Pakistan.
[2]Bacha Khan University, Charsadda, 24420, Pakistan.
[3]Higher Colleges of Technology, Dubai, UAE.
[4]Iqra National University, Peshawar, 25000, Pakistan.
[5]Pak-Austria Fachhochschule Institute of Applied Sciences and Technology, Haripur, Pakistan.
[*]Corresponding Author: M. Imran Khan Khalil. Email: imrankhalil@uetpeshawar.edu.pk

Academic Editor: Salman Qadri **Published:** April 01, 2024

Abstract: The Internet of Things (IoT) has seamlessly integrated into various aspects of our daily lives, spanning wearable devices, biomedical, agricultural, and industrial applications, among others. With the evolution of every device comes the convenience of remote access and cloud computing. However, this interconnectedness also exposes personal and sensitive data to potential attacks on confidentiality, integrity, and availability. This paper delves into the broad spectrum of security challenges faced by IoT, emphasizing the urgency of addressing these issues. Furthermore, we shed light on various research avenues that could offer solutions to the security dilemmas plaguing IoT. Questions arise regarding the efficacy of domain-independent security patterns in developing secure IoT systems and the existence of IoT security-supporting architectures. Our objective is to conduct a comprehensive analysis of existing literature on patterns and designs for IoT security. Adhering to established protocols for systematic reviews, we aim to provide insights into this critical research area, facilitating the advancement of secure IoT systems.

Keywords: Internet of Things (IoT); Security Challenges; Security Architecture; Confidentiality; Domain-independent Patterns.

1. Introduction

In the foreseeable future, it is predicted that billions of electronic devices will be interconnected via the Internet of Things (IoT), aiming to enhance productivity with minimal human intervention [1], [2]. Various sectors such as agriculture, healthcare, automation, and smart grids are generating terabytes of data daily, which are transmitted to the cloud. However, this transmitted data contains private and critical information that must be safeguarded from unauthorized access, ensuring integrity, confidentiality, and accessibility [3], [4], [5]. Despite the existence of numerous secured and complex security schemes, IoT data remains vulnerable due to challenges such as computational complexity for small-scale IoT devices, limited power resources for remote devices, and onboard storage constraints [6], [7].

The concept of IoT has been prevalent for several decades, even before it gained widespread recognition in the early 2010s. Prior to this, IoT devices and applications were utilized to a limited extent across various societal sectors. Leveraging internet protocols, IoT facilitates the integration of devices, data, and applications, leading to the development of a wide array of IoT applications across industries [8], [9].

One significant sector embracing IoT is the consumer IoT, which introduces wearable technology equipped with sensors for activity and health tracking [10-12].

In the healthcare sector, IoT applications and devices play a pivotal role in monitoring and improving healthcare services. These include robotic surgery, efficient drug management, glucose monitoring, remote patient monitoring, and augmented reality headsets, among others. However, vulnerabilities in IoT security pose risks not only to data but also to human health and lives, as seen in cases where internet-connected pacemakers are used to manage cardiac rhythms [13], [14].

The proliferation of IoT devices in the market, although beneficial, introduces challenges due to resource limitations. These challenges exacerbate existing security concerns and introduce new ones, stemming from factors such as device heterogeneity and inter-device communication. Security issues in IoT are categorized into networking, hardware, and software limitations, each presenting distinct challenges [15], [16]. Hardware constraints include compute, storage, power, and memory limitations, while software constraints relate to embedded software limitations. Networking limitations encompass mobility, scalability, and intermittent network connections, exacerbated by low-power transceivers with low data rates [17].

The security challenges posed by IoT are further compounded by the diverse nature of connected devices and their communication protocols. Insecure design of applications and programs, along with the large number of IoT devices, increase the complexity of security issues, making them more intricate to address [18], [19-23]. The heterogeneity of communication media introduces additional security hindrances, necessitating comprehensive security measures to ensure connectivity and accessibility of devices.

Furthermore, IoT field devices operate in dynamic execution contexts with limited data transport and storage capabilities, rendering IoT systems inherently unreliable. Given the significant security and privacy challenges associated with IoT, our research aims to explore the patterns and architectures deployed in this domain. We seek to identify existing security patterns and algorithms designed for IoT security and privacy, analyze gaps in current state-of-the-art solutions, and propose strategies to enhance security and privacy in contemporary IoT systems [24], [25].

2. Systematic Literature Review Approaches

In this section, we outline our comprehensive systematic literature review (SLR) approach, which encompasses planning, conducting, and reporting stages. Our aim is to thoroughly investigate patterns and architectures for IoT security and privacy, addressing key research questions and providing in-depth insights into existing literature.

2.1. Research Area Identification

The foundation of our SLR lies in identifying the research area and formulating relevant research questions [26]. We aim to explore the landscape of IoT security and privacy, specifically focusing on patterns and architectures. The following research questions guide our investigation:

- RQ1: What studies have been conducted on patterns and architectures for IoT security and privacy?
- RQ2: What are the technical specifications of these security patterns and architectures in the context of IoT security and privacy?
- RQ3: How can security patterns and architectures be effectively adapted for the Internet of Things, and what gaps exist in current research?

2.2. Inclusion and Exclusion Criteria

To ensure the comprehensiveness and relevance of our review, we establish clear inclusion and exclusion criteria [27]. Included studies must:

- Focus on patterns and architectures for IoT security and privacy
- Provide insights into security aspects specific to IoT environments
- Present findings related to technical specifications, adaptation, and gaps in existing research 3

Exclusion criteria may include studies unrelated to IoT security, those lacking depth or relevance, and non-peer-reviewed sources.

2.3. Search Strategy and Selection Process

We employ a systematic approach to search for relevant literature across multiple databases, including academic journals, conference proceedings, and online repositories. Keywords related to IoT security, patterns, architectures, and privacy are used to identify potential studies [28], [29]. The selection process involves screening titles, abstracts, and full texts to ensure alignment with inclusion criteria. Additionally, citation chaining and reference list checks are conducted to identify additional relevant studies [30-36].

2.4. Data Extraction and Synthesis

Data extraction involves systematically collecting information from selected studies, including research title, publication details, research type, methodology, techniques, and key findings related to IoT security patterns and architectures [37]. Synthesizing extracted data involves organizing and summarizing findings, identifying common themes, and highlighting trends, advancements, and gaps in the literature. Comparative analysis and critical appraisal of study methodologies are conducted to assess the quality and reliability of research findings [38].

Table 1. Data extraction and characteristics

Characteristics	Questions
Research Title, Publication, Research Type	What studies focus on patterns and architectures for IoT security?
Area of research, Methodology, Techniques	What are the technical specifications of these patterns and architectures?
New methods, Advancements, Shortcommings	What gaps exist in IoT security based on the findings of these studies?

2.5. Reporting and Analysis

The reporting stage involves synthesizing findings into a comprehensive narrative, structured according to research questions and themes identified during data synthesis [39]. Detailed descriptions of included studies, their methodologies, key findings, and implications are provided. Analytical insights and interpretations are presented to offer a nuanced understanding of the research landscape, including strengths, limitations, and future directions [40].

2.6. Limitations and Considerations

It is essential to acknowledge potential limitations of the SLR, such as publication bias, language restrictions, and the evolving nature of IoT security research. Methodological considerations, such as the reproducibility of search strategies and the rigor of data extraction, are also addressed to enhance the credibility and trustworthiness of our review [41].

In summary, our comprehensive SLR approach aims to provide a detailed exploration of patterns and architectures for IoT security and privacy. By systematically analyzing existing literature, we seek to

contribute valuable insights to the field, inform future research directions, and support the development of effective security solutions for IoT environments.

3. Literature Review

The Internet of Things (IoT) has ushered in a new era of connectivity and convenience, with billions of devices seamlessly communicating and interacting with each other. However, this interconnectedness also brings forth a myriad of security challenges that threaten the integrity, confidentiality, and availability of IoT systems. To address these challenges, it is essential to understand the landscape of IoT security and the complexities involved. This literature review aims to provide a comprehensive overview of the challenges facing IoT security, exploring various aspects such as threats, vulnerabilities, privacy concerns, network security challenges, regulatory issues, supply chain risks, and human factors.

3.1. Security Threat Landscape

The IoT security threat landscape is diverse and constantly evolving, with attackers exploiting vulnerabilities to launch a wide range of attacks. Common threats include malware, ransomware, distributed denial-of-service (DDoS) attacks, data breaches, and unauthorized access. These threats pose significant risks to IoT devices, networks, and data, highlighting the need for robust security measures [42].

3.2. Vulnerabilities in IoT Devices

IoT devices are often characterized by resource constraints, limited processing power, and minimal security features, making them vulnerable to exploitation. Common vulnerabilities include insecure firmware, default credentials, lack of encryption, and inadequate update mechanisms. Attackers can exploit these vulnerabilities to gain unauthorized access to devices, compromise data integrity, and launch cyberattacks [43].

3.3. Privacy Concerns

Privacy is a major concern in the IoT ecosystem, as the proliferation of connected devices leads to the collection, processing, and sharing of vast amounts of personal and sensitive data. Issues such as data leakage, unauthorized surveillance, and profiling raise significant privacy concerns among users. Moreover, the lack of transparency and control over data collection and usage exacerbates these concerns, necessitating robust privacy protections [44], [45].

3.4. Network Security Challenges

IoT networks are heterogeneous and decentralized, comprising a diverse array of devices, protocols, and communication technologies. This heterogeneity introduces challenges in network security, such as interoperability issues, protocol vulnerabilities, and lack of standardization. Additionally, the dynamic nature of IoT environments poses challenges in network management and access control [46].

3.5. Regulatory and Compliance Issues

The regulatory landscape surrounding IoT security is complex and fragmented, with varying standards and regulations across different jurisdictions. Compliance with regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) poses challenges for IoT stakeholders. Moreover, the rapid pace of technological innovation often outpaces regulatory frameworks, creating gaps in security and compliance [47], [48].

3.6. Supply Chain Risks

The supply chain ecosystem for IoT devices is vast and interconnected, spanning multiple vendors, manufacturers, and service providers. This complexity introduces supply chain risks, such as counterfeit components, tampering, and supply chain attacks. Ensuring the integrity and security of the supply chain is crucial to mitigating these risks and safeguarding IoT systems against compromise [49].

3.7. Human Factors

Human factors play a significant role in IoT security, as user behavior and awareness can impact the security posture of IoT systems. Factors such as poor password management, lack of security awareness, and susceptibility to social engineering attacks contribute to security vulnerabilities. Educating users and fostering a security-conscious culture are essential for enhancing the resilience of IoT systems [50].

In conclusion, the Internet of Things presents a multitude of security challenges that require careful consideration and proactive measures to address. From vulnerabilities in IoT devices to privacy concerns, regulatory issues, and supply chain risks, navigating the security maze requires a comprehensive understanding of the threats and risks involved. By identifying these challenges and exploring potential solutions, this literature review contributes to the ongoing discourse on IoT security and informs future research and development efforts.

4. IOT Security Threats

The Internet of Things (IoT) has become an integral part of daily life, revolutionizing how we interact with technology. However, along with its numerous benefits, IoT also poses significant threats to privacy and security, both directly and indirectly. In this section, we delve into the main threats to IoT security and their implications.

4.1. Confidentiality Threats

Confidentiality threats revolve around the inadvertent disclosure of private information. Sensitive data may be exposed due to breaches in confidentiality within IoT monitoring systems. For example, knowledge of the operating parameters of an air conditioning system and seemingly innocuous information such as interior temperature can be leveraged to determine whether a property is occupied. Breaches in confidentiality can also lead to risks of unauthorized system access through the compromise of keys and passwords [51].

4.2. Integrity Threats

Integrity threats concern the preservation and assurance of data accuracy and completeness throughout its lifecycle. Ensuring data integrity is crucial to maintaining trust and reliability in IoT systems. Any compromise in data integrity can lead to misinformation or manipulation, jeopardizing the functionality and reliability of IoT applications [52].

4.3. Authentication Threats

Authentication threats pose risks of unauthorized manipulation of control or sensor data. For instance, unauthenticated system status alerts may deceive a home controller into believing that an emergency has occurred, prompting actions such as opening doors and windows for emergency evacuation. However, these actions may inadvertently grant unauthorized entry. Authentication mechanisms play a critical role in verifying the identity of users and ensuring the integrity of data exchanges in IoT systems [53].

4.4. Access Threats

Access threats represent one of the most significant risks to IoT security. Unauthorized access to system controllers, particularly by administrative personnel, can compromise the entire system's security. This unauthorized access may result from poor key and password management practices or the connection of unauthorized devices to the network. Unauthorized network connections can lead to bandwidth theft or denial-of-service attacks, disrupting legitimate IoT operations [54], [55].

We conduct a comprehensive analysis of primary studies focusing on the aforementioned threats to IoT security and privacy. By examining the implications of these threats and their potential impact on IoT

ecosystems, we aim to provide insights into effective mitigation strategies and best practices for safeguarding IoT environments. Through our analysis, we seek to contribute to the ongoing discourse on IoT security and support the development of robust security frameworks for the future of IoT technology.

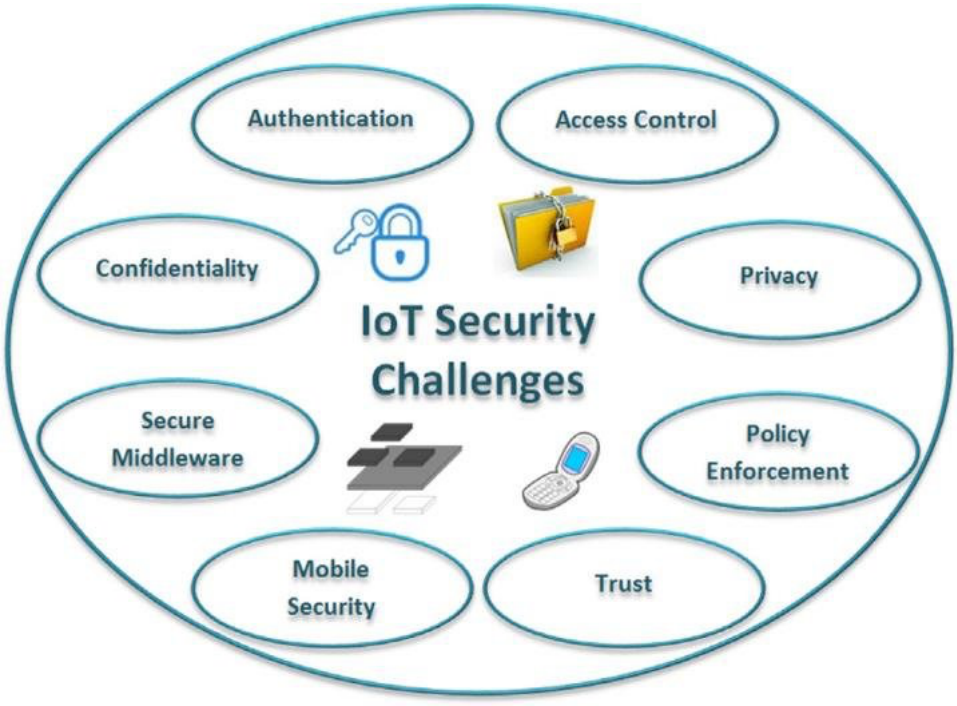

Figure 1. IoT Security Challenges

5. Results and Discussion

The systematic literature review (SLR) conducted in this study provides valuable insights into the landscape of IoT security and privacy architectures. This section presents the findings of the SLR and discusses the implications of the identified trends and research contributions.

5.1. Trends in IoT Security Publications

The analysis of primary studies revealed a significant increase in research publications focusing on IoT security and privacy architectures over the past decade. This trend indicates a growing recognition of the importance of addressing security challenges in IoT ecosystems. The publications were categorized into conferences and journals, with the majority of research areas centered around IoT, 5G, network, and security technologies. Notably, the number of security challenges and architectures publications in conferences surpassed those in journals by more than double by the year 2024.

5.2. Contributions to IoT Security

The primary studies reviewed in this SLR made valuable contributions to the field of IoT security and privacy. These contributions encompassed various aspects, including real-life case studies, experimental testing, and proposed solutions. For instance, one study [13] highlighted the detrimental effects of Distributed Denial-of-Service (DDoS) attacks on IoT systems and proposed mitigation strategies. Another study [14] proposed a blockchain-based architecture pattern to enhance data provenance and integrity, as well as hardware security measures using cryptographic co-processors [15]. Additionally, a study [16] focused on securing human life in smart cities while preserving citizen privacy.

5.3. Discussion

The findings of this SLR underscore the increasing importance of addressing security challenges in IoT ecosystems. While the number of publications in this area has grown significantly, the analysis suggests that research on IoT security patterns and designs is still in its early stages. This highlights the need for further development and exploration in both academic and industrial domains.

One of the key challenges identified is the lack of awareness and expertise in IoT security among developers. This can lead to vulnerabilities and breaches in IoT systems, particularly in scenarios where developers are under time-to-market pressure. Security patterns emerge as a potential solution to mitigate this lack of understanding, offering domain-independent, time-proven security knowledge and skills. By integrating security patterns early in the development process, developers can address security constraints effectively and minimize the risk of malicious usage.

However, several challenges remain in the application of security patterns and architectures in IoT environments. Compatibility and complexity issues, as well as the heterogeneity of communication protocols, pose significant hurdles. While existing patterns address general and specific security issues, there is a lack of systematic approaches for their application. Future research should focus on addressing these gaps and developing comprehensive frameworks for the systematic integration of security patterns in IoT systems.

In conclusion, the findings of this SLR highlight the need for continued research and innovation in IoT security. By addressing existing challenges and leveraging security patterns effectively, stakeholders can enhance the resilience and security of IoT ecosystems, paving the way for the widespread adoption of IoT technologies in various domains.

6. Future Directions

While this systematic literature review (SLR) has provided valuable insights into the current state of IoT security and privacy architectures, there are several avenues for future research and development in this field. Addressing the following areas can contribute to the advancement of IoT security and enhance the resilience of IoT ecosystems.

6.1. Development of Comprehensive Security Frameworks

Future research should focus on developing comprehensive frameworks for IoT security that encompass various aspects such as authentication, encryption, access control, and intrusion detection. These frameworks should provide guidance on the integration of security measures across different layers of the IoT stack and offer best practices for mitigating emerging threats.

6.2. Enhancement of Security Patterns

Security patterns play a crucial role in addressing common security challenges in IoT systems. Future work should involve the refinement and expansion of existing security patterns to cover a broader range of use cases and scenarios. Additionally, efforts should be made to develop domain-specific security patterns tailored to specific IoT applications and industries.

6.3. Integration of Artificial Intelligence (AI) and Machine Learning (ML)

AI and ML techniques have the potential to enhance the security capabilities of IoT systems by enabling proactive threat detection and adaptive response mechanisms. Future research should explore the integration of AI and ML algorithms for anomaly detection, behavior analysis, and predictive maintenance in IoT environments.

6.4. Standardization and Interoperability:

The lack of standardization and interoperability in IoT security protocols and mechanisms poses significant challenges. Future work should focus on developing standardized security protocols and

interoperability frameworks that facilitate seamless communication and collaboration between diverse IoT devices and platforms.

6.5. Privacy-Preserving Technologies

With the increasing concerns surrounding data privacy in IoT ecosystems, future research should explore privacy-preserving technologies that enable secure and confidential data sharing and processing. Techniques such as homomorphic encryption, differential privacy, and secure multi-party computation can help protect sensitive information while enabling meaningful data analytics and insights.

6.6. End-User Education and Awareness

Improving end-user education and awareness is essential for fostering a security-conscious culture in IoT environments. Future work should involve the development of educational resources, training programs, and awareness campaigns aimed at educating IoT users about potential security risks and best practices for safeguarding their devices and data.

6.7. Collaborative Research and Industry Partnerships

Collaborative research initiatives involving academia, industry, and government stakeholders can accelerate progress in IoT security research and development. Future work should encourage interdisciplinary collaboration and industry partnerships to address real-world security challenges and validate proposed solutions in practical IoT deployments.

By addressing these future research directions, stakeholders can advance the state-of-the-art in IoT security and privacy, mitigate emerging threats, and build a more secure and trustworthy IoT ecosystem for the future.

References

1. Mrabet, H.; Belguith, S.; Alhomoud, A.; and Jemai, A. "A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis," Sensors, 2020, vol. 20, no. 13, p. 3625.
2. Kumar, G. E. P.; Lydia, M. and Levron, Y. "Security Challenges in 5G and IoT Networks: A Review," Secure Communication for 5G and IoT Networks, 2022, vol. 5, no. 3, pp. 1–13.
3. Tawalbeh, L.; Muheidat, F.; Tawalbeh, M. and Quwaider, M. "IoT Privacy and Security: Challenges and Solutions," Applied Sciences, 2020, vol. 10, no. 12, p. 4102.
4. Hossain, M.M.; Fotouhi, M.; and Hasan, R. Towards an analysis of security issues, challenges, and open problems in the Internet of Things, 2015 IEEE World Congress Serv., 2015, pp. 21–28.
5. Meng, Y.; Zhang, W.; Zhu, H.; Shen, X.S. "Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures" IEEE Wireless Communication, 2018, vol. 25, no. 5, pp. 53–59.
6. Khan, A.; Aziz, S.; Bashir, M.; and Khan, M. U. "IoT and Wireless Sensor Network based Autonomous Farming Robot," 2020 International Conference on Emerging Trends in Smart Technologies (ICETST), Karachi, Pakistan, 2020, pp. 1-5.
7. Yeh, K. H. "A Secure IoT-Based Healthcare System With Body Sensor Networks," in IEEE Access, 2016, vol. 4, pp. 10288-10299.
8. Madakam, S.; Ramaswamy, R.; and Tripathi, S. Internet of Things (IoT): a literature review, J. Computing and Communication, 2015, vol. 3, no. 5, pp. 234-355.
9. Hasan, M. "IoT in healthcare: 20 examples That'll make you feel better," April 2, 2020. [Online]. Available: https://www.ubuntupit.com/iot-in-healthcare-20- examples-thatll-make-you-feel-better. [Accessed: Nov. 5, 2020].
10. Zhang, Z. K.; Cho, M. C. Y.; Wang, C. W.; Hsu, C. W.; Chen, C. K. and Shieh, S. "IoT Security: Ongoing Challenges and Research Opportunities," 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, Matsue, Japan, 2014, pp. 230-234, doi: 10.1109/SOCA.2014.58.
11. Sicari, S.; Rizzardi, A. and Coen-Porisini, A. "5G In the internet of things era: An overview on security and privacy challenges," Computer Networks, 2020, vol. 179, p. 107345.
12. Lee, H. "Home IoT resistance: Extended privacy and vulnerability perspective," Telematics and Informatics, 2020, vol. 49, no. 3, p. 101377.
13. Pahl C, Ioini NE, Helmer S, Lee B "An architecture pattern for trusted orchestration in iot edge clouds. In: 2018 third international conference on fog and mobile edge computing (FMEC), 2018, pp 63–70. https:// doi. org/ 10. 1109/ FMEC. 2018. 83640 46.
14. Witti, M.; Konstantas, D. "A secure and privacy-preserving internet of things framework for smart city. In: Proceedings of the 6th international conference on information technology: IoT and smart city. ICIT 2018. Association for Computing Machinery, New York, NY, USA, 2018, pp. 145–150. https:// doi. org/ 10. 1145/ 33015 51. 33016 07
15. Zhao, Z.; Resnick, P.; and Mei, Q. "Enquiring minds: Early detection of rumors in social media from enquiry posts," in WWW 2015 - Proceedings of the 24th International Conference on World Wide Web, May 2015, pp. 1395–1405.
16. Zubiaga, A.; Aker, A.; Bontcheva, K.; Liakata, M.; and Procter, R. "Detection and resolution of rumours in social media: A survey," ACM Computing Surveys, 2018, vol. 51, no. 2, pp. 210-225.
17. Khalil, M. I. K.; Afsheen, A.; Taj, A.; Nawaz, A.; Jan, N.; and S. Ahmad, "Enhancing Security Testing Through Evolutionary Techniques: A Novel Model" Journal of Computing & Biomedical Informatics, 2023, vol. 6, no. 1, pp. 375 – 393.
18. Li, M.; Wang, X.; Gao, K.; and Zhang, S. "A survey on information diffusion in online social networks: Models and methods," Information, MDPI, 2017, vol. 8, no. 4.
19. Camargo, D.; and Popov, S. "Total Flooding Time and Rumor Propagation on Graphs," J Stat Phys, 2017, vol. 166, no. 6, pp. 1558–1571.
20. Khalil, M. I. K. and Taj, T. "Factors Affecting the Efficacy of Software Development: A Study of Software Houses in Peshawar, Pakistan," International Review of Basic and Applied Sciences, 2021, vol. 9, no. 3, pp. 385-393.
21. Zhang, K., Zheng, Y., and Yang, Q. "Detection of Rumors in Social Media". In Proceedings of the 24th ACM International Conference on Multimedia, 2016, pp. 797-798.
22. Ma, J., Gao, W., and Wong, K. F. "Detect Rumors in Microblog Posts Using Propagation Structure via Kernel Learning" IEEE Transactions on Cybernetics, 2015, vol. 45, no. 11, pp. 2447-2458.
23. Khalil, M. I. K. Ullah, A.; Taj, A.; Khan, I.A.; Ullah, F.; Taj, F.; and Shah, S. "Analysis of Critical Risk Factors Affecting Software Quality: A Study of KPK, Pakistan Software Industry," International Review of Basic and Applied Sciences, 2022, vol. 10, no. 2, pp. 338-348.
24. Wu, L., Zhang, J., Wang, X., and Lu, X. "A Novel Two-Stage Rumor Detection Framework", In Proceedings of the 27th International Conference on Computational Linguistics, 2015, pp. 3402-3412.
25. Jin, Z., Cao, K., and Zhang, H. "A Feature-based Approach for Rumor Detection in Social Media" Information Processing & Management, 2020, vol. 53, no. 1, pp. 165-177.
26. Saqib, A.; Ullah, M.; Hyder, S.; Khatoon, S.; and Khalil, M. I. K. "Creative Decision Making in Leaders: A Case of Beer Game Simulation," Abasyn Journal of Social Sciences, 2020, vol. 12, no. 2, pp. 379-387.
27. Liu, Y., Zhang, R., and Song, H. "Rumor Detection on Social Media with Graph-based Deep Learning", Neurocomputing, 2021, vol. 337, no. 5, pp. 41-49.

28. Khan, I.A; Ullah, F.; Abrar, M.; Shah, S.; Taj, F. and Khalil, M.I.K. “Ransomware Early Detection Model using API-Calls at Runtime by Random Decision Forests,” International Review of Basic and Applied Sciences, 2022, vol. 10, no. 2, pp. 349-359.
29. Gupta, A., Kumaraguru, P., and Castillo, C. “Credibility Ranking of Tweets during High Impact Events”, In Proceedings of the 2014 ACM Conference on Web Science, 2014, pp. 172-181.
30. Zhou, X., Zhang, L., Huang, R., and Liu, C. “Dissecting Rumors: Analyzing and Predicting Rumor Patterns on Twitter”, ACM Transactions on Information Systems (TOIS), 2016, vol. 34, no. 3, pp. 1-27.
31. Jan, S.; Maqsood, I.; Ahmad, I.; Ashraf, M.; Khan, F. Q.; and Khalil, M. I. K. "A Systematic Feasibility Analysis of User Interfaces for Illiterate Users," Proceedings of the Pakistan Academy of Sciences, 2020, vol. 56, no. 4, pp. 2518-4253.
32. Giasemidis, G., and Papadopoulos, S. “Rumor Detection in Social Media Streams.” In Proceedings of the 12th International Conference on Availability, Reliability and Security, 2019, pp. 1-8.
33. Khalil, M. I. K.; Shah, S. A. A.; Khan, I. A.; Hijji, M.; Shiraz, M.; and Shaheen, Q. “Energy cost minimization using string matching algorithm in geo-distributed data centers,” Computers, Materials, and Continua, 2023, vol. 75, no. 3, pp. 6305-6322.
34. Kumar, S., Morstatter, F., and Liu, H. “Twitter Data Analytics”, Springer, 2018, vol. 4, no. 2, pp. 25-33.
35. Zhao, Z., Resnick, P., and Mei, Q. “Enquiring Minds: Early Detection of Rumors in Social Media from Enquiry Posts”, In Proceedings of the 24th International Conference on World Wide Web, 2015, pp. 1395-1405.
36. Wu, H., Fang, H., and Lei, J. “Bursty Rumor Detection in Social Media”, Knowledge-Based Systems, 2022, vol. 118, no. 3, pp. 35-44.
37. Ahmad, I.; Khalil, M. I. K.; and Shah, S. A. A. "Optimization-based workload distribution in geographically distributed data centers: A survey," International Journal of Communication Systems, 2020, vol. 33, no. 12, p. e4453.
38. Gupta, A., and Kumaraguru, P. “Credibility Ranking of Tweets during High Impact Events”, In Proceedings of the First Workshop on Privacy and Security in Online Social Media, 2019, pp. 1-10.
39. Jambudi, B., and Kumar, K. “Machine Learning Approach for Detecting Rumors in Social Media. Procedia Computer Science”, 2016, vol. 132, no. 5, pp. 1431-1438.
40. Khalil, M. I. K.; Ahmad, I.; Shah, S. A. A.; Jan, S.; and Khan, F. Q. "Energy cost minimization for sustainable cloud computing using option pricing," Sustainable Cities and Society, 2020, vol. 63, p. 102440.
41. Kwon, S., Cha, M., Jung, K., Chen, W., and Wang, Y. “Prominent Features of Rumor Propagation in Online Social Media”, In Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 2013. pp. 461-468.
42. Khalil, M. I. K.. “Improve quality of service and secure communication in mobile adhoc networks (MANETS) through group key management,” International Review of Basic and Applied Sciences, 2013, vol. 1, no. 3, pp. 107-115.
43. Li, H., Wang, W., Li, F., and Zhao, Y. “A Survey of Rumor Detection Methods on Social Media”, ACM Computing Surveys (CSUR), 2023, vol. 52, no. 3, pp. 1-36.
44. Muhammad, D.; Ahmad, I.; Khalil, M. I. K.; Khalil, W.; and Ahmad, O. A. “A generalized deep learning approach to seismic activity prediction,” Applied Sciences, MDPI, 2023, vol. 13, p. 1698.
45. Gupta, A., Kumaraguru, P., and Castillo, C. “TweetCred: Real-time Credibility Assessment of Content on Twitter”, In Proceedings of the 22nd International Conference on World Wide Web, 2016, pp. 635-636.
46. Shu, K., Sliva, A., Wang, S., Tang, J., and Liu, H. “Fake News Detection on Social Media: A Data Mining Perspective”, ACM SIGKDD Explorations Newsletter, 2021, vol. 19, no. 1, pp. 22-36.
47. Khalil, M. I. K. “Job satisfaction and work morale among Ph.D’s: A study of public and private sector universities of Peshawar, Pakistan,” International Review of Management and Business Research, 2013, vol. 02, no. 2, p. 362.
48. Ahmad, I.; Ahmad, M. O.; Alqarni, M. A.; Almazroi, A. A.; and Khalil, M. I. K. "Using algorithmic trading to analyze short-term profitability of Bitcoin," PeerJ Computer Science, 2021, vol. 7, p. e337.
49. Chen, T., and Guestrin, C. “XGBoost: A Scalable Tree Boosting System”, In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2018, pp. 785-794.
50. Khalil, M. I. K.; Shah, S. A. A.; Taj, A.; Shiraz, M.; Alamri, B.; Murawat, S.; and Hafeez, G. “Renewable aware geographical load balancing using option pricing for energy cost minimization in data centers,” Processes, MDPI, 2022, vol. 10, no. 10, p. 1983.
51. Gupta, A., and Kumaraguru, P. “Credibility Ranking of Tweets during High Impact Events”, In Proceedings of the First Workshop on Privacy and Security in Online Social Media, 2012, pp. 1-10.
52. Khalil, M. I. K.; Ahmad, A.; Almazroi, A.A. “Energy Efficient Workload Distribution in Geographically Distributed Data Centers,” IEEE Access, 2019, vol. 7, no. 1, pp. 82672-82680.
53. Wu, B., Wei, W., Sun, W., and Huang, Y. “An Improved Algorithm for Rumor Detection Based on Machine Learning”, Future Generation Computer, 2021, vol. 37, no. 3, pp. 88-101.
54. Khalil, M. I. K..; Mubeen, A.; Taj, A.; Jan, N.; Ahmad, S. “Renewable and Temperature Aware Load Balancing for Energy Cost Minimization in Data Centers: A Study of BRT, Peshawar,” Journal of Computing & Biomedical Informatics, 2023, vol. 06, no. 3, pp. 1-8.
55. Anum, H.; Khalil, M. I. K..; Nawaz, A.; Jan, N.; and Ahmad, S. “Enhancing rumor detection on social media using machine learning and empath features,” Journal of Computing & Biomedical Informatics, 2023, vol. 06, no. 2, pp. 6-13.