https://doi.org/10.29042/2020-10-4-51-58

Helix (2020) 10 (4): 51-58

Cloud Computing and Security in the IoT Era

[1] Yahya Abssi, [2] Shailendra Mishra, [3] Manoj Kumar Shukla

[1]Department of Information Technology, College of Computer & Information Sciences, Majmaah University, Majmaah-11952, Saudi Arabia

391104182@s.mu.edu.sa

[2]Department of Computer Engineering, College of Computer & Information Sciences, Majmaah University, Majmaah-11952, Saudi Arabia

s.mishra@mu.edu.sa

[3]Department of Electronics Engineering, Harcourt Butler Technical University, Kanpur

mkshukla@hbtu.ac.in

Received: 22nd June 2020, Accepted: 03rd July 2020, Published: 31st August 2020

Abstract

Advancements in information technology, and transfer of data online leading to the vulnerabilities and giving an invitation to cyber threats. Security and privacy are important issues in cloud storage and networking fields. Cloud computing created an environment that facilitates the internet of things. The cloud computing technology consisted of servers, applications, and other storage devices, relying on the virtual connection. The stored information in clouds can be manipulated without the need for extensive physical activities. The internet of things devices provide information and services through information and communication technology, these end-node IoT devices are not very intelligent and resource-constrained thus they are vulnerable to cyber threats. It posed an issue of insecurity as malicious individuals learned ways of intruding these systems and causing intellectual and physical losses. The study proposes numerous solutions for the challenges of privacy and security in the cloud and IoT. The paper provides an in-depth examination of security challenges in cloud computing and IoT. The methodology uses the interpretive technique. The results depict the importance of the machine and deep learning in cyber-attack and mitigation. Analysis of variance (ANOVA) test statistics is used to test the reliability of the study.

Keywords

Cloud Computing, Internet of Things, Privacy Concerns, Servers, Security

Introduction

The internet of things (IoT) ranks high as an outstanding archetype in the 21st century undoubtedly. The first impression of the term would suggest that it means connecting things through the internet. This technology developed through the cloud computing (CC) foundation; CC devices provide the platform needed to enhance and expand IoT to the world [1,2]. Nevertheless, some security concerns continue to derail the expansion of the CC-IoT systems into all parts of human life, these concerns dwell in the realm of cybersecurity with questions such as privacy intrusion rising. Irrespective of how wonderful the technology continues to become with matters of application intelligence and data analytics, the query of how to sufficiently protect information emerges most of the time [3]. Companies and even government store uses enormous amounts of data on clouds. For ease of use the servers used in the processes are invaluable to many people. These factors attract malicious parties to attack and extract information [4].

The security issues are among the biggest worries in companies that rely on cloud computing to do business; the management of the businesses state that unauthorized activities affect the flow of business. Moreover, the risk increases when the company outsources these cloud storage services through the use of a vendor [5]. Third-party vendors in cloud computing are a common practice in the corporate world, all the companies are at least if the vendor suffers from security breaches [6,7].

Many organizations shifting to the cloud, critical business applications, and massive quantities of critical data could now exist in systems available from anywhere across the globe. The system is accessible not only to customers and employees, but also to potential cybercriminals [9]. Environmental subtleties are also disrupting and changing resiliency with the speedy adoption of cloud set-up and the spread of IoT gadgets. The idea of a border is vanishing, and the fight against cybercrime has drifted inside the system, with this change, organizations require to reconsider their security.

This research answers these questions; a connection between access control in cloud computing and privacy in the modern world, the security measures when it comes to cloud computing, the impact of the internet of things and cloud computing connect in the digital era, what are the technical processes predominant in the cloud-based security protocols? The study proposes numerous solutions for the challenges of privacy; these include anti-malware, firewall, intrusion prevention systems, and hardware authentication. The reliability of the study was tested using ANOVA statistical method.

 Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

The work in this paper is organized in a different section, an introduction gives the overall concept of research to be conducted, background and related work are discussed in second. The research methodology is discussed in section three, result analysis and discussion are discussed in section four, finally, research findings and future aspects of this research are discussed in the conclusion.

Background

Cloud computing (CC) continues to revolutionize the way people communicate and conduct their businesses. Companies such as Microsoft, Google, Apple, and Amazon continues to use cloud computing in their commercial activities [10]. The biggest derailment in the advancement of cloud computing is the insecurity of data. Many companies fear extensive use of cloud computing because of the implied security risk in the contemporary era. The information or systems which operate on the web face the vulnerability of attacks from malicious parties [11,12]. The connection of the internet with an embedded computer system coupled with sensors and actuators brought about the notion of the IoT. Another definition of the IoT comes from Joy's six Webs taxonomy, which shows that the technology is part of the sixth classification called D2D or device-to-device web [13,14].

The world of IoT coincides with the field of cloud computing. The internet of things permits connection between smart and non-smart systems through the application of the internet [15]. Cloud computing allows users of these systems to use servers, applications, and other forms of storage [16]. The cloud storage occurs within the premise or off-premise depending on the service provider and the client. The narrative affirms the comprehensive relationship between IoT and cloud computing. However, one of the challenges of these two technologies is vulnerability to hacking or lack of privacy. It means that the issue of privacy and information is mechanically out of the reach of the human client [17,18].

The internet of things possesses the similar challenges of security as would cloud computing. The growing market for IoT also attracts malicious individuals trying to gain access to the marketplace. These individuals target weak computers in the world and use them to conduct their illegal activities [19]. The study of the internet of things in [20], shows great merits and concerns, especially with the growing vulnerability and the flexibility of moving data back and forth through IoT makes it ideal. Also, describe the various layers of IoT such as the application layer and network layer, and scrutinize the specific security issues affecting each layer. The authors affirm that the application layer suffers from authentication issues while the network suffer from connectivity and security issues.

The current technological environment accommodates the demands of cloud computing and the internet of things. According to the paper [21], the world of IoT thrives in the modern century because of its versatile use in many industries. IoT is instrumental in, revenue growth, cost reduction, and monetizing customer data through the delivery of value-added services [22]. The advancement in cloud computing and various applications of networking system makes it easy to incorporate into company operations. This assertion showing that the trend spreads into the international economy and plays key roles in many operations. This fact means that insecurity affects many companies across the globe and needs further attention [22]. Additionally, the Internet of Things advanced the normal computer systems characterized by software and its implementation [23]. Six key features when it comes to secure IoT/ cloud computing namely, “authentication, confidentiality, redundancy, data freshness, anonymity & misuse, and liability”, These parameters are vital for a perfectly functioning system [24]. In the paper [25,26] authors discussed vulnerabilities resulting in brute force attack, Man-in-the-Middle (MITM) attack, social engineering, and Advanced Persistent Threats, ARP poisoning, DHCP starvation, and countermeasures.

The development of cloud computing provides both commercial and individual benefits to users. In [27] authors describe how technology aids in both industrial automation and other fields of the economy. The application is diverse given that cloud computing laid the structural foundation for IoT in the 21st century. The related-work provides a variety of sources for referencing; they use prototype testing, modeling, and simulation together with the informational qualitative analysis. Other localized solutions were antimalware, firewall, intrusion prevention systems, and hardware authentication. The company utilizing cloud computing should invest in these forms of security measures because abandoning the whole system is inconceivable because of its implied merits [28].

In paper [29,30], authors provided solutions through an examination of current systems CC and IoT based on 5G and present an inclusive view of the structure of these technologies and challenges. The assessment focuses on the connection between the internet of things (IoT) and cloud computing, together with the challenges and solutions given in the contemporary era. The study presented in [31] gives an elaboration of about nine sources diving deep into the architecture of the network systems and how they are susceptible to threats from malicious individuals or groups. The diversity assists in developing a credible and unbiased understanding of security issues in cloud computing and IoT. The results prove that the technical structure of cloud storage leaves loopholes which malicious parties can use to access and sabotage the work of a company; it leads corporations to rethink their security protocols and come up with advanced means of guarding their assets. Most of these articles focus on using advanced security measures which only companies can afford. The literature would help individuals understand the benefits of cloud computing to individuals and how they can protect their gadgets such as cell phones and personal computers.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

Research Methodology

The methodology utilizes the interpretive perspective of gaining information. Multiple case studies, research papers, questionnaires, and the use of digital interviews from experts will aid in the investigation and gathering of information. Topics covered are cloud computing security, IoT, cyber security, privacy and trust, issues, challenges and possible countermeasures, some queries may demand a deliberate attempt to associate IoT with cloud computing. The research methods consist mainly of qualitative tactics of extracting information through questionnaires, discussion and interviews. The participants will give a personal account of the experiences with various security systems and their reaction to how security breaches occur frequently in their industry. The research objectives were explained and a questionnaire sent to 80 experts in the field of cloud computing & IoT. The response rate was 75%.

Questions used are;

1. What is the trend in the frequency of privacy breaches over the last decade or so?
2. How many privacy breaches can you remember off-head from 2010 onwards?
3. Weightage of important factors affecting the adoption of cloud and IoT based application.
4. Do you think there is any technological solution effective in curbing insecurity?
5. How does wireless and sensor networks help stop or progress the era of insecurity?
6. Are there any human-based interventions for insecurity found in the company?
7. Should the company just rely on technological discoveries alone?

The interviews aid in addressing the abstract aspects of cloud computing and any associated field. The structured interview consisting of several questions touching different topics associated with the research objectives. The method permits freedom between interviewee and interviewer together with a deeper assessment of the situation. This research technique allows the team to not only get responses to the questionnaire content but also to see the emotions and memories associated with the technology first-hand. Case studies in this scenario involve reading through articles with the same topic and seeing their conclusions. This methodology aids in exploring all perspectives of the security issues without remaining closed out in a particular region or industry. Case studies will provide a more concrete framework for the results of the interview, it allows for a definite derivative of security issues in the research field. ANOVA statistical test techniques were used and the NCSS data analysis tool [32] was used to test the normality and reliability of the data.

Results and Analysis

The experimental analysis and evaluation explore the results of empirical study and checks whether the findings coincide with the related work articulates. The framework of the experiment seeks to observe both subjective and objective views of participants in the questions dealing with insecurity. The interviews provide an opportunity for the researcher to extract both verbal and non-verbal cues concerning the evolution of cloud computing security in the last decade and the efficiency of the security measures used nowadays. The results show that incidents of insecurities increased over the years and companies need to develop a complex means of tackling privacy breaches.

Increased Frequency of Security Breaches

Among the many questions asked in interviews and questionnaires was the frequency of breaches in the modern world. The participants revealed that the number of security breaches has increased from as far as 2010. The question involved asking how many breaches they can remember off the head in their industries in the respective years and the answers were compiled and placed in a graph as shown in Fig,1. The blue line shows the progress of years, while the orange indicates the frequency in each year. The trend indicates that breaches increase with time. The advancement of technology was the principal reason identified by participants as the main contributor to malicious attacks.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

Fig. 1: Increase in Frequency of Security Breaches

Questions asked regarding factors that can be influencing the adoption of cloud and IoT based technology

F1: Trust, Security, and Privacy
F2: Fast Attack detection and mitigation using Machine learning (ML) and deep learning (DL)
F3: The importance of Firewall, IDS, IPS
F4: Resource utilization policies
F5: Service level Agreement
F6: Load Balancing using ML and DL
F7: Low maintenance and operation cost

93% participants acknowledged on factor F1, 92 % participants acknowledged on F2, 90 % acknowledged on F3, 89 % acknowledged on F4, 82% of respondents acknowledged on F5,82% of respondents acknowledged on F6, 70 % of respondents acknowledged on F7, Fig. 2, depicts the importance of security factor in the adoption of cloud base application, also the importance of machine learning and deep learning in cyber-attack detection and mitigation. Overall 93 % believed that security protocols could help eliminate all the issues with privacy and confidentiality. The results were eye-opening given that most of the participants were working in the information technology sector. Only 7 % of the participants asserted that technology was not enough to solve problems; human misconduct could still cause issues with privacy and confidentiality. Results explore how the current technology of machine learning is essential in information security. Deep learning allows for similar advantages of concise treatment of diseases and storage of information together with the ability to optimize non-differentiable discontinuous loss functions. The importance of firewall, IDS, anti-malware, firewall, intrusion prevention systems, and hardware authentication.

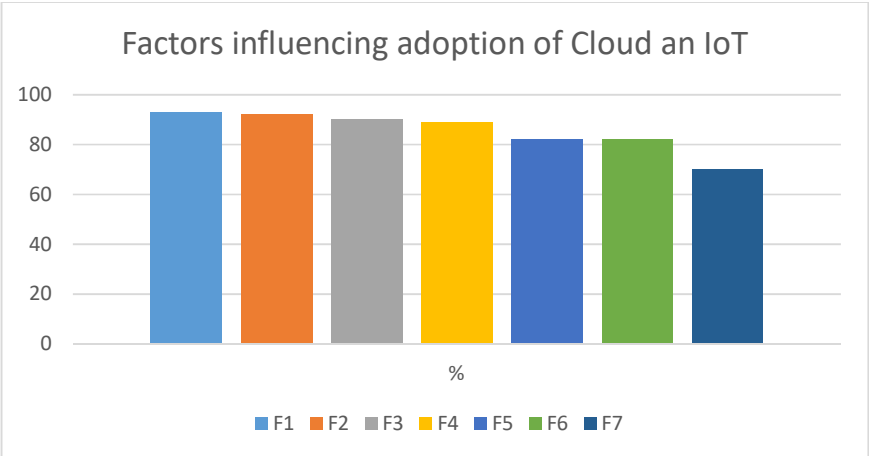

Fig. 2: Factors influencing the Adoption of Cloud and IoT

 Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

The input of individuals working within the cloud storage industry proves that security protocols are necessary; they emphasize the use of human behavior analytics to complement the digital system used to guarantee privacy. The results of the study provide solutions to the privacy and confidentiality challenges along with the necessary information about how cloud storage is vulnerable to attack and how they can guard against any future intrusion.

Reliability and Normality Analysis

Reliability and Normality Analysis was tested using ANOVA test statistic.

The reliability of the study is tested using Cronbach Alpha (α), where Alpha (α) is the probability of rejecting the null hypothesis Significance level $\alpha = 0.05$.

Factors that can be influencing the adoption of cloud and IoT based technology are;

F1: Trust, Security, and Privacy

F2: Fast Attack detection and mitigation using Machine learning (ML) and deep learning (DL)

F3: Importance of Firewall, IDS, IPS

F4: Resource utilization policies

F5: Service level Agreement

F6: Load Balancing using ML and DL

F7: Low maintenance and operation cost

The hypotheses of interest in an ANOVA are as follows:

H0: All medians are equal.

H1: At least two medians are different.

The test value of Skewness is close to zero, and the value of Kurtosis is zero means the data set is normally distributed

[33,34].

Table 1: Tests of the Normality

Normality Attributes	Test Value	Probability Level	Reject Normality? (α=0.2000000000)
Skewness	0.000000006	0.0000000400	No
Kurtosis	0.0000000000	0.0000000800	No

This research study is reliable since in all cases, Cronbach Alpha (α) lies between 0.79 and 0.94 (or higher in some cases) [35,36].

Table 2: Reliability Analysis

Variable/Factors	Experts IT Industry (N=60)
	Cronbach Alpha
F1	0.9552
F2	0.9454
F3	0.9358
F4	0.8765
F5	0.8588
F6	0.8563
F7	0.8463

Discussion

A detailed study is conducted to support the research and leading towards the findings. A research methodology is developed which highlights the factors have been impacting and analyzed these factors with the study of security models and their implementation and finally, their impacts have been discussed. Mobile and web systems are widespread in the current tech-world. The internet of things provides a baseline for all these trends. Experts in the fields encourage app development and the provision of immediate outcomes for the clients. The shift guarantees a convenient and quick delivery of services in their homes. The government regulation and issues of privacy breaches hamper the efforts of the IT experts. The use of artificial intelligence techniques such as machine learning alleviates the burden. The problem of appropriate regulation of such a venture creates doubts about its reliability. The benefits of technology become practical when using 5G technology in industrial IoT to give off better outcomes. The assertion proves that technology growth is the foundation of development in the modern age.

Deep learning and machine learning are a great addition to the cloud computing era. Deep learning fits well with the Internet of Things wave. Both technologies use sensors and actuator systems for automation and accommodate

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

data generation. Using smart transit structures for devices can help solve issues of privacy breaches in the industries. Moreover, IoT security helps in protecting the details of patients and clients. The operations under this category require less human players as opposed to conventional systems. Deep learning and IoT has a robust security protocol that reduces privacy y breaches and improves the industry.

Cyber-Security affects every sector of the economy and underlines the need for more research and innovation. Data is streamed across new and numerous channels in the modern age. More so, transmission occurs everywhere with the growth and advancement of technology. Therefore, issues of security and data protection are a core factor in all business transactions across the globe. The process involves the collection of data, processing to make useful information, and storage through automated mechanisms. The storage results in developing a database for filing. In effect, it adheres to safeguarding the right to privacy, which transcends regional and international conventions, and laws. Its purpose is to maintain Data integrity, confidentiality, and availability. Furthermore, confidentiality pertains to data being hidden from unauthorized people; this means that only allowed individuals should access it.

This security requirement can be achieved in two ways. First, strong authentication policy, when accessing any data. Integrity is attained by the use of algorithmic data validation. Algorithms such as checksum and one-way hashes are used. Nevertheless, regardless of whether the data is altered maliciously or by accident preventing that change is of utmost concern, and its detection the second. All these requirements are vital for companies to access data in a safe environment irrespective of physical location and time. The availability of information is another crucial goal of cybersecurity. Accidents or attacks may bring a system down. The same data might be deleted, destroyed, or overwritten. Alternatively, access and retrieval of data become slow instead of complete restrictions. Subsequently, cybersecurity has become so intrinsic in organizations and individuals. Data protection requirements involve the provision of policies and compliances for handling and protection at various levels of its lifecycle; the cycle continues from its conception, storage, translation to information up to its ultimate destruction/deletion if need be. Comparatively, it encompasses security standards required for electronic devices used to store or access the data. Conclusively, the information lifecycle of data includes the collection, access, sharing, storage, auditing, sending, and destruction. As a result, the requirement of storage of data applies to both the source and copies if any made to any number of devices.

Data exists in several different formats digitally and is classified as internal Data, restricted-use data and confidential, each of which as different requirements. Some of these classifications are only applicable to business and organizational institutions since they are more vulnerable to threats. The requirements for the three classifications require a situation where there is no restriction on internal data collection. However, access to sensitive information requires the provision of credentials on company devices. The sharing of this type of data with employees requires departmental approval. Sequentially, the channels should adhere to pre-determined authentication codes when sending the data. Another security is the implementation of a secure email service for privacy. Periodical auditing should be conducted concerning the location of data, access to history, and the control mechanisms. Incident reports of data loss and unauthorized access must be reported to the proper parties.

Devices on the network are considered part of data systems hence systems security controls are implements for their protection. Measures are placed to stop inbound unauthorized access to the firewalls and prevent access control lists, etc. Instructions, detection services, and technology should be deployed to monitor inbound and outbound traffic to prevent data breaches. Other measures taken to secure data include establishing strong passwords on systems where data is stored. This may be done by combining capital and lowercase letters, symbols, and numbers; that should be 8 characters and more. These passwords should be changed regularly. Password management tools should also be used for due diligence. Finally, restriction of access to those management tools should be limited to authorized users, set up firewalls to protect the network by controlling data transfer to and from the internet. The installation of anti-virus is a fundamental arsenal against online defense weapons. Update programs and patch software utilities regularly. Encryption of data is not widely used despite data encryption technology being one of the most recent talked topics in the information technology industry. Moreover, the tactic is useful in protecting sensitive data. The encryption will vary based on the level of applicable threats, device performance, and interoperability of the data storage environment.

Conclusions

Cloud computing denotes technology used for virtual storage of information, while the Internet of Things assets to the connection of items through the internet. These two technologies are vital for modern business. The IoT platform evolved from the foundation of the capabilities of cloud computing; both technologies lead to improved corporate and personal operations. However, the same technologies suffer from insecurity; their design of existing through cyberspace makes them susceptible to hacking and other privacy issues. The possibility of complete confidentiality is nonexistent. Companies must invest in better digital systems and upgrade them regularly to prevent vulnerabilities. Cloud computing promotes communication through peer-to-peer connections and is highly convenient for uses across the globe. These same network systems are accessible to individuals with malicious intentions. As a result, information security continues to grow as an emergent and an necessary aspect

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

of modern technology. The study proposes numerous solutions for the challenges of privacy; these include anti-malware, firewall, intrusion prevention systems, and hardware authentication. Anti-malware encompasses software used to guard against viruses and spyware among other harmful applications. It lowers the possibility of malware attacking applications on computers or the network. Hardware authentication is another solution that works well for cloud computing applications, users must undergo certain security steps before accessing their accounts or the database.

The future work can be extended by accessing documents of government institutes and big organization and from the enterprise documents to make the research more precise and more detailed oriented. Artificial intelligence is an area gaining momentum in the current century and it proves to be a solution to many problems that the world face, especially in security and manufacturing sectors.

References

[1] Zamora-Izquierdo, M. A., Santa, J., Martínez, J. A., Martínez, V., & Skarmeta, A. F. (2019). Smart farming IoT platform based on edge and cloud computing. Biosystems engineering, 177, 4-17.

[2] Yousefpour, A., Fung, C., Nguyen, T., Kadiyala, K., Jalali, F., Niakanlahiji, A., ... & Jue, J. P. (2019). All one needs to know about fog computing and related edge computing paradigms: A complete survey. Journal of Systems Architecture, 98, 289-330.

[3] Albdour, L., Manaseer, S., & Sharieh, A. (2020). IoT Crawler with Behavior Analyzer at Fog layer for Detecting Malicious Nodes. Int. J. Commun. Networks Inf. Secur., 12(1).

[4] Kumari, P. L. S. (2020). Big Data: Challenges and Solutions. In Security, Privacy, and Forensics Issues in Big Data (pp. 24-65). IGI Global.

[5] S. Mishra, S. K. Sharma and M. A.Alowaidi, "Analysis of security issues of cloud-based web applications," Journal of Ambient Intelligence and Humanized Computing, https://doi.org/10.1007/s12652-020-02370-8, 2020.

[6] Gozman, D., & Willcocks, L. (2019). The emerging Cloud Dilemma: Balancing innovation with cross-border privacy and outsourcing regulations. Journal of Business Research, 97, 235-256.

[7] Shah, J. L., Bhat, H. F., & Khan, A. I. (2019). Cloud IoT: Towards Seamless and Secure Integration of Cloud Computing With Internet of Things. International Journal of Digital Crime and Forensics (IJDCF), 11(3), 1-22.

[8] Cheng, B. H., Doherty, B., Polanco, N., & Pasco, M. (2019, September). Security Patterns for Automotive Systems. In 2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C) (pp. 54-63). IEEE.

[9] Rychwalska, A., Goodell, G., & Roszczynska-Kurasinska, M. (2019). Data management for platform-mediated public services: Challenges and best practices. Available at SSRN 3455123.

[10] Cusumano, M. A. (2019). The cloud as an innovation platform for software development. Communications of the ACM, 62(10), 20-22.

[11] Dizdarevic, J., Carpio, F., Jukan, A., & Masip-Bruin, X. (2019). A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration. ACM Computing Surveys (CSUR), 51(6), 1-29.

[12] Jouini, M., & Rabai, L. B. A. (2019). A security framework for secure cloud computing environments. In Cloud security: Concepts, methodologies, tools, and applications (pp. 249-263). IGI Global.

[13] Tewari, A., & Gupta, B. B. (2020). Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Future generation computer systems, 108, 909-920.

[14] Ahmed, A. I. A., Ab Hamid, S. H., Gani, A., & Khan, M. K. (2019). Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open research challenges. Journal of Network and Computer Applications, 145, 102409.

[15] Norouzi, N., Bruder, G., Belna, B., Mutter, S., Turgut, D., & Welch, G. (2019). A systematic review of the convergence of augmented reality, intelligent virtual agents, and the internet of things. In Artificial Intelligence in IoT (pp. 1-24). Springer, Cham.

[16] Jamali, M. A. J., Bahrami, B., Heidari, A., Allahverdizadeh, P., & Norouzi, F. (2020). IoT Security. In Towards the Internet of Things (pp. 33-83). Springer, Cham.

[17] Singh, V., & Pandey, S. K. (2020). Cloud Computing: Vulnerability and Threat Indications. In Performance Management of Integrated Systems and its Applications in Software Engineering (pp. 11-20). Springer, Singapore.

[18] Domingo-Ferrer, J., Farràs, O., Ribes-González, J., & Sánchez, D. (2019). Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges. Computer Communications, 140, 38-60.

[19] Jalali, M. S., Kaiser, J. P., Siegel, M., & Madnick, S. (2019). The Internet of Things Promises New Benefits and Risks: A Systematic Analysis of Adoption Dynamics of IoT Products. IEEE Security & Privacy, 17(2), 39-48.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

[20] Darwish, A., Hassanien, A. E., Elhoseny, M., Sangaiah, A. K., & Muhammad, K. (2019). The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems. Journal of Ambient Intelligence and Humanized Computing, 10(10), 4151-4166.
[21] Shim, J. P., Avital, M., Dennis, A. R., Rossi, M., Sørensen, C., & French, A. (2019). The transformative effect of the internet of things on business and society. Communications of the Association for Information Systems, 44(1), 5.
[22] Barralon, P., Charrat, B., Chartier, I., Chirie, V., Fico, G., Guillen, S., & Peine, A. (2019). IoT for smart living environments: recommendations for healthy ageing solutions.
[23] Sanin, C., Haoxi, Z., Shafiq, I., Waris, M. M., de Oliveira, C. S., & Szczerbicki, E. (2019). Experience based knowledge representation for Internet of Things and Cyber Physical Systems with case studies. Future Generation Computer Systems, 92, 604-616.
[24] Jamali, M. A. J., Bahrami, B., Heidari, A., Allahverdizadeh, P., & Norouzi, F. (2020). IoT Security. In Towards the Internet of Things (pp. 33-83). Springer, Cham.
[25] Brenner, B., & Weippl, E. (2019). Security Analysis and Improvement of Data Logistics in AutomationML-Based Engineering Networks. In Security and Quality in Cyber-Physical Systems Engineering (pp. 305-334). Springer, Cham.
[26] Brenner, B., & Weippl, E. (2019). Security Analysis and Improvement of Data Logistics. Security and Quality in Cyber-Physical Systems Engineering: With Forewords by Robert M. Lee and Tom Gilb, 305.
[27] Jia, M., Komeily, A., Wang, Y., & Srinivasan, R. S. (2019). Adopting Internet of Things for the development of smart buildings: A review of enabling technologies and applications. Automation in Construction, 101, 111-126.
[28] Attaran, M., & Woods, J. (2019). Cloud computing technology: improving small business performance using the Internet. Journal of Small Business & Entrepreneurship, 31(6), 495-519.
[29] Appio, F. P., Lima, M., & Paroutis, S. (2019). Understanding Smart Cities: Innovation ecosystems, technological advancements, and societal challenges. Technological Forecasting and Social Change, 142, 1-14.
[30] Varga, P., Peto, J., Franko, A., Balla, D., Haja, D., Janky, F., ... & Toka, L. (2020). 5g support for industrial iot applications–challenges, solutions, and research gaps. Sensors, 20(3), 828.
[31] Costin, A., Wehle, A., & Adibfar, A. (2019). Leading indicators—a conceptual IoT-based framework to produce active leading indicators for construction safety. Safety, 5(4), 86.
[32] (NCSS,2020) NCSS: Statistical Software (www.ncss.com) /accessed on 6 March 2020.
[33] Qu, W., Liu, H., & Zhang, Z. (2019). A method of generating multivariate non-normal random numbers with desired multivariate skewness and kurtosis. Behavior Research Methods, 1-8.
[34] Bono, R., Arnau, J., Alarcón, R., & Blanca, M. J. (2020). Bias, precision, and accuracy of skewness and kurtosis estimators for frequently used continuous distributions. Symmetry, 12(1), 19.
[35] Mishra, S., & Singh, M. (2019). A Conceptual framework for effective M-Governance. Journal of Engineering Science and Technology, 14(6), 3514-3535.
[36] Kong, Y., Wang, Y., Hajli, S., & Featherman, M. (2019). In sharing economy we trust: Examining the effect of social and technical enablers on millennials' trust in sharing commerce. Computers in Human Behavior, 105993.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495