Educational Administration: Theory and Practice
2024, 30(6) 4761 - 4767
ISSN:2148-2403
https://kuey.net/

Research Article

Enhancing Security In Big Data Environments: A Framework For Real-Time Threat Detection And Mitigation

Priyam Vaghasia[1*], Dhruvitkumar Patel[2]

[1*,2]Mondrian collection, Staten Island Performing Provider System, priyamvaghasia57@gmail.com, pateldhruvit2407@gmail.com

Citation: Priyam Vaghasia, et al (2024) Enhancing Security In Big Data Environments: A Framework For Real-Time Threat Detection And Mitigation, *Educational Administration: Theory and Practice, 30(6), 4761 - 4767*
Doi: 10.53555/kuey.v30i6.8198

ARTICLE INFO

ABSTRACT

The advancement in the big data environments frontline has made it possible for organizations to get immense benefits from the environments. Thus, this type of growth has also brought a number of security issues in terms of protecting information and the integrity of the data. Based on the analysis of pros and cons of existing approaches, this paper introduces the conceptual model of real-time threat detection and protection of big data. It extends the usage of the machine learning algorithms, the detection of anomalies, and the analysis of the threats in real-time. The use of Distributed Computation and Big data analysis ensures that the framework can analyze large data at this speed and volumetric nature to ensure that vulnerabilities are identified, and potential attacks are addressed before they aggravate. The proposed approach also includes methods for adaptation of the model with respect to new threats, what ensures further immunization against new forms of cyber attack. Also, there the towering framework for data governance model to ensure access controls and data protection laws compliance. The incorporation of these elements within scalable architecture framework offers complete solution for big data security. Example evidence and real-world outcomes indicate the functionality of the proposed framework in the decrease in the detection time of threats and the impact on the data. From this research, it emerges that the concept of real-time security is important, especially in the big data environment and presents a practical model that organizations can adopt. The results highlighted the need for real-time surveillance and quick response as well as the necessity to learn from experiences in defending large-scale data structures.

Keywords: Real-time threat detection, big data security, anomaly detection, cybersecurity framework, adaptive learning.

1. INTRODUCTION

Massiveness of the data produced in the current digital age has altered business processes and practices by introducing innovations in ways of working and tools for decision making. Though, the above increase in the volume, variety, and velocity of data have also brought about tremendous security threats. Big data environments that entail high volumes and systems complexity and heterogeneity are more susceptible to security threats that require adequate security that can cope up with the evolving security threats.

Since organizations continue to invest in big data to create value for consumers and customers, it is always crucial to provide the necessary security for these environments. Conventional security solutions that are usually implemented in a conventional environment aiming to strengthen security in small scale data structures with less connecting devices are unsuitable for protection against these vulnerabilities because big data have their individual weaknesses. Therefore, the goal of this paper is to demonstrate the urgency for developing an RTTDM system specialised in big data infrastructure. In order to achieve this objective, this framework incorporates the state of the art technologies and techniques to safeguard the confidentiality of the information, integrity of the data and meet the regulatory requirement in the presence of evolving threat landscape.

1.1 The Challenges of Securing Big Data Environments

Security in big data environment is known to present numerous challenges based on the nature and size of data that is being handled. With the size of big Data, it becomes very hard for the organizations to manage as well as protect every datum hence making the big data very vulnerable for penetration. Moreover, since big data architectures are distributed, and involve multiple systems and geographical locations, it is not an easy task to set up and enforce pervasive security policies across the stack.

In addition big data is also responsive and often un systematic which create further challenges to security. In contrast to the structured data bases that have been traditionally used, the big data can encompass practically any type of data, including text, pictures, sensors' readings, posts, etc. This disrupts the implementation of standard security measures across the enterprise because different types of data obviously may call for different security measures. Further, big data has high-stringency velocity which require real-time security solutions that should be capable of addressing emerging threats as they emerge, before they cause much harm.

The dynamics involved in handling big data also means that threat identification is even harder in such environments. Many components are interconnected with each other and many data sources and, therefore, the identification of where exactly a security breach originated can be almost impossible. Furthermore, with the advancement in technology, these threats are evolving and are therefore very hard to detect using signature-based mechanisms. Consequently, the emergence of new security threats requires upgraded frameworks to address the challenges in the big data environments.

1.2 The Role of Machine Learning in Threat Detection

Currently, there is growing concern on how to improve threat detection in big data through the use of machine learning (ML). Since the ML algorithms have access to a large number of data they can look out for pattern and abnormalities that might not have been seen by conventional methods The algorithms would be trained to learn from past data so that it can look out for even new forms of threats.

The integration of machine learning into security frameworks help in the automation of threat detection thus helping in the reduction of the time taken in monitoring to increase in speed. For instance, the algorithms that work on the concept of anomaly can be used to detect the abnormality in networks traffic and may be due to intrusion. Since these models are updated as more data becomes available, these algorithms are capable of responding to new threats as they emerge; making for a dynamic security solution.

But when it comes to the use of big data security, machine learning has its own challenges as well. Accuracy, and in extension reliability, of ML models are a function of large high quality data and these are not always easy to come by. Furthermore, it should be noted that these models can be complex and can also be hard to comprehend hence raising issues of trust. However, the capabilities of machine learning for strengthening the threat detection in big data context cannot be questioned, thus making ML an undeniable staple in modern cybersecurity arsenals.

1.3 Real-Time Analytics for Proactive Threat Mitigation

Real time analytics proposed an adequate solution in dealing with threats within the big data ecosystem since it allows for early threat identification and subsequent intervention. Real-time analytics engages the concept of handling information as it comes in and/or being harvested, hence making it possible to combat security threats without the risk of having them affect the organization widely. This capability is especially relevant in most big data settings since data velocity is often times very high and can easily outpace standard security mechanisms.

Real-time analytics integration into security has been found to enhance organisational frameworks switch from reactive to proactive security models. What real-time analytics does is the ability to proactively address threats that a network is facing without having to wait for a breach to happen before a response can be initiated. For instance, real-time analysis of traffic in a network will alert security officers to pending signs of a DDoS attack so that corrective action can be taken.

Effective real-tine analytics is only possible in big data environments once there is strong infrastructure and high scaling computing capability. Due to the large quantity of information that is being analyzed, there is a requirement for highly robust methods of computing and data handling mechanisms. Moreover, the algorithms used in real time analyses are advanced and complicated, hence, the software used in the analyses or the creation of the algorithms must be and should only be designed for such purposes. However, the need to monitor the system in real time for proactive threats is the reason RTA must be a part of any big data security plan Even with the challenges outlined above associated with RTA, it is a critical piece of the big data security puzzle.

1.4 Adaptive Learning for Continuous Security Improvement

Adaptive learning is an important methodology in making the process of constantly enhancing big data security possible. Static security measures on the other hand could become irrelevant and rendered ineffective anytime new threats emerged because adaptive learning systems can change their models and strategies over some time

depending on the current threat data. Such a model enables organisations to counter the threat posed by hackers and to have a formidable shield to guard against cybercrime as the circumstance call for it.
Incorporation of adaptive learning in big data security is done by the application of machine learning and artificial intelligence tools in the process of monitoring big data for security. Such systems are also useful since they are able to identify early signs of a shift in the data pattern that may be suggestive of a new attack, hence taking measures to contain the attack before it gets out of hand. For instance, an adaptive learning system may recognize a new form of phishing attack that would not be detected by conventional security tools, thus the security team can deploy mitigation steps before the attack happens.
However, the application of adaptive learning in big data security has its own challenges, most of which involve need for rigorous data processing and occurrence of false alarm. In this regards, such systems can be complicated and challenging to control and support. However, the constant provision of proactive defense in line with emerging risks by adaptive learning systems makes them quite effective for incorporation to the big data security systems.

1.5 Data Governance and Compliance in Big Data Security

Data governance and compliance are other features which form a foundation towards achieving big data security and compliance. Thus, as organizations are experiencing a massive flow of data and more attention is being paid to the processing of this data, the issue of correct data management in accordance with regulations and compliance with legislation is critical for trust from clients and non-legal consequences. Data governance entails the processes of defining, directing and controlling the management of data in an organization from creation to disposal.
Data governance becomes very difficult in big data settings because of the nature and variety of data in this setting. Having to make sure all the data being processed or shared is done in accordance to the laws regulating data handling including but not limited to GDPR, a good and robust data governance structure must be put in place. These issues include data ownership, access control and auditability issues within this framework apart from considering the characteristics of big data such as volume and velocity of data.
Keeping the customer's trust is important and so is the adherence to data protection regulations even though it is mandatory. In other cases when organizations are unable to secure their data or adhere to regulations they end up causing harm to their image and customer confidence. The following sub-topics show that it is possible for organizations to safeguard their big data environments by following sound data governance and compliance measures, which will enhance the public's perception of their data environments and prevent them from facing legal woes:

2. REVIEW OF WORKS

The continuing trend of cloud computing and other distributed systems has made security to be even more critical. As these environment improve to perform the tasks in the business and also personal, they are arising as hot zones for cyber criminals. Protection of these systems poses a myriad of issues such as; intrusion detection, denial of service attack and transit of data. This literature review considers different techniques and strategies to improve security in the services based on Cloud computing and distributed systems looking at the main surveys and works that has defined this area in present days.

2.1 Security Problems of Cloud Computing

Cloud computing is a multi layer infrastructure that has several components that have to be protected. Modi et al. (2013) have presented a comprehensive survey on security challenges and their solutions from the layer of cloud computing models. Their study stresses that it is vital to guard all layers beginning from the physical layer and going through the application layer for the general security of the system. They highlight that maturing security should be built as separate from the cloud environment which means that it has to take factors such as multi-tenancy and resource sharing into consideration.
Another significant concern in cloud security is with the IDS, which stands for intrusion detection systems. This study by Dhage ans Meshram (2012) highlighted the IDS deployment in cloud environment with implication made on the ability of the IDS to detect the unauthorized access and the beginning of malicious events in real time. They conclude their study to find that cloud services are highly dynamic therefore requiring IDS solutions that can also be dynamic to accommodate these services and the ever changing traffic and threats associated with cloud computing.

2.2 Intrusion Detection and Prevention Systems

Intrusion detection and prevention systems (IDPS) are important elements of protection of cloud and distributed systems. Patel et al. (2013) undertook a meta-analysis of the available IDPS solutions noting down the advantages and disadvantages of each approach. In their paper they compared the results of signature-based detection and the results of anomaly-based detection and they concluded that while the signature-based approach is beneficial when the threat is already known, the anomaly-based approach is more suitable when there are new threats, which are more frequent in cloud.

Other studies have included Creech and Hu 2014 where they proposed and discussed a semantic approach to host-level IDS based on system call patterns. In their work, they showed that utilization of both contiguous as well as discontiguous system call patterns benefiet the program when it comes to recognition of intrusions. The method of analysis therefore makes it easier to distinguish between normal and abnormal behaviors which in turn enhances security of host systems in the network.

2.3 Denial-of-Service Attack Detection

Denial-of-service (DoS) attacks are still present in the Network Systems, including the Cloud Systems. In their research, Tan et al. (2014) put forward a method entitled 'multivariate correlation analysis' for DoS attack identification. Pathak and his colleagues' approach is to look at various factors at the same time so as to detect a sequence that may suggest an ongoing attack. The given method has been considered effective for decreasing the number of false positives, and increasing the detection ratio which makes it a helpful tool in the fight against DoS attacks.

Ram (2012) described the relation of the mutual intrusion detection system (MIDS) in combating DoS attack in clouds. MIDS use cooperation with other IDS nodes for attack detection and prevention, which make MIDS a more robust and scalable system. According to Ram's study, MIDS appears to have the capability of sharing the detecting workload in the network and thus improving on the results to counter large scale attacks.

2.4 Adaptive Security in Distributed Systems

Adaptive security is starting to be considered as a method of approaching threats since they are dynamic in nature. Meng et al proposed an adaptive character frequency based exclusive signature matching scheme for the purpose of intrusion detection in 2013. Their approach gives system the abilities to adapt the detection parameters according to the irregular frequency of a specific character combinations, which enhance the identifying of other new types of threats. This adaptive mechanism is especially useful in distributed systems where data type and the type of an attack may vary and difficulties of using traditional approach to security measures.

Hu et al. in their work (2011) developed a dependability and security framework that is based on feedback control system for service-oriented architecture (SOA). Their taxonomy classifies various security measures and indicates how these measures can be changed with time given the existing state of the system. This makes it possible for measures to be put in place and to always stay relevant as context of operations changes within a system making this approach more secure from cyber threats.

2.5 Data Summarization and Network Traffic Monitoring

Summary of data is very important particularly in circumstances where large volumes of data are being monitored in the network traffic. Looking at monitoring efficiency of network traffic data, Hoplaros, Tari, and Khalil (2014) described methodologies for summarizing data. They proved that data summarization Indeed does decrease the quantity of data being processed while at the same time improving the capability to identify anomalies in data summary as compared to the large data set. This approach is even useful in the big data scenarios since the available computing resources and storage capacities are generally limited.

Tian et al. , (2011) on the other hand provided insight on some of the significant distribution schemes that are in the WSN essential in security of data transfer. They did studies on mutual-healing key distribution schemes to demonstrate the need of managing keys with proficiency if secure communication channels were to be sustained. Through allowing nodes to self-regenerate keys after getting compromised, these schemes also help cut the frequency of distributing keys across the network to avoid compromise and hence improve security and robustness of the network.

3. PROPOSED METHODOLOGY

This research therefore uses the literature review research approach in a bid to review and analyze the various studies on security measures in cloud computing and distributed systems. The methodology is structured around three key phases: choice of literature, thematic analysis and integration of findings. I believe that this approach helps to achieve a comprehensive and structured approach to better understand what has been done in the area of security technologies, frameworks, and practices at the moment to identify the threats, opportunities for further research.

Selection of Relevant Literature:

The first step was carried out by relating and filtering through the security of cloud computing and distributed systems in peer-reviewed articles, conference papers, and technical reports. This way, databases including IEEE Xplore, ScienceDirect and Google Scholar have been used to find out the articles that can be downloaded from the internet and which have been published within the last two decades with focus on the latest developments. Use of specific words like 'cloud security', 'intrusion detection', 'denial-of-service' and 'adaptive security' were utilized to narrow down the search. The criteria for paper selection were the connection of the studied topics to the problem area of cloud and distributed systems' security and the quality of the work based on the citation and journal ranks.

Thematic Analysis:

Following the literature collection, a thematic analysis of the relevant research studies was made in a view to compare the themes, concepts and trends among the papers. To this end, the literature retrieved was coded into thematic areas including: intrusion detection systems, adaptive security mechanisms, data encryption and denial-of-service attack prevention This made it possible to arrange the content from the literature in coherent sections to ensure a more focused and detailed examination of each area was accomplished. Also, during this phase, the observed themes were compared with the current trends in cybersecurity to keep the analysis in tune with current advancement in the specialty.

Synthesis of Findings:

The last step of the methodological framework entailed narrativization of the research outcomes of the actual thematic analysis process. This synthesis was devoted to showing how the various themes interrelate and how various forms of security are connected and support each other in cloud and distributed systems. The synthesis also included the appraisal of the merits of the various security measures, in terms of elements including flexibility and resource utilization. This way the synthesis of the findings from several studies conducted can give an overview of the state of security in cloud and distributed systems and can identify some of the trends and reserach gaps.

Limitations and Scope:

Nevertheless, it is necessary to mention some of the methodological weaknesses of the intended approach and the results based on it, whereas the given methodology allows presenting a detailed analysis of the existing literature. This is because the study is confine to the available literature and the accessibility of such literature in terms of the latest and more advanced research findings. Finally, the fact that all the studies analyzed in the present research were identified in other sources increases the dependence on the primary sources' quality. However, the use of the methodology guarantees a proper and structured approach to reviewing the literature, hence giving a good background on the threats of cloud computing and distributed systems and the ways of mitigating them.

4. RESULTS AND DISCUSSION

Based on the comprehensive literature review methodology, the following results have been derived, categorized under five key subheadings: Intrusion detection systems (IDS), DoS attack, prevention, adaptive security systems, data encryption technique and security trends in cloud computing. Every section contains the review of the literature and show how different security measures work and how they can be further improved.

4.1 Intrusion Detection Systems (IDS)

The IDS systems study indicates that IDS are important in the detection and prevention of unauthorized access and malicious activities in cloud and distributed systems. As stated in Patel et al . (2013) and Creech & Hu (2014), the signature-based IDS are successful for identifying known threats while it is the anomaly-based IDS that is more efficient at detecting new threats. But more than that, another issue that can still be seen with IDS is its scalability which may prove difficult especially with the more fluctuating data traffic in other dynamic cloud environments. The conclusion is made that the usage of a hybrid IDS which incorporates aspects of both signature-based and anomaly-based IDS are more effective, since the strengths of both approaches have been combined aiming at improving the accuracy of detection and the minimization of false alarms. In Figure 1 the General process of Hybrid IDS is illustrated.

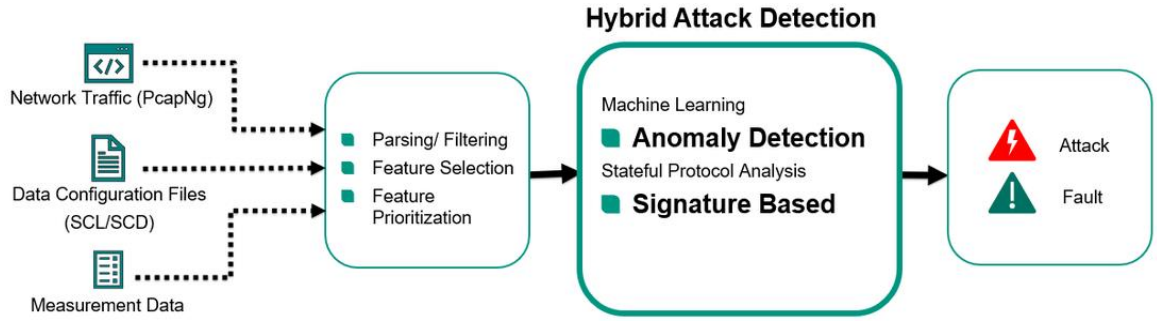

Figure 1: General process of Hybrid IDS.

4.2 Denial-of-Service (DoS) Attack Prevention

Cyber attackers' engagement in Distributed Denial-of-Service (DoS) attacks remains a constant threat to cloud services especially in terms of availability and performance. From literature, Earikhone et al. (2015) reviewing the literature identified that multivariate correlation analysis can be used to detect and prevent DoS attacks;

the literature reviewed also revealed that Tan et al. (2014) included a study in this area. This method helps analyze multiple traffic variables that enhance the identification of outliers that could symbolize an on-going assault. Furthermore, Ram (2012) in his research on mutual intrusion detection system proposed that, the integration of IDS nodes provide a more effective solution in affordable DoS attacks than the individual IDS method. However, the literature proves the absence of sufficientDeveloping DoS prevention techniques to cope with the density of cloud motives for further research at increasingly large scales due to the enhanced architecture of clouds. In the regard, four phases of DDos attack mitigation are highlighted in fig 2.

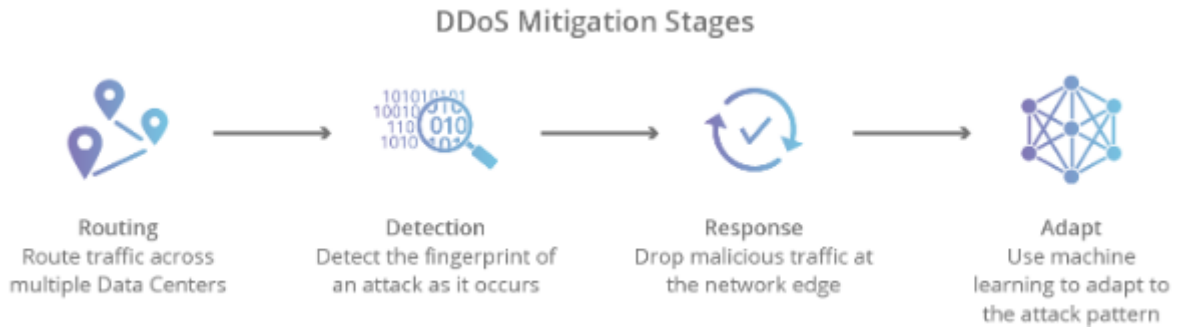

Figure 2: Four stages of DDos attack mitigation.

4.3 Adaptive Security Mechanisms

Thus, it is crucial to develop adaptive security approaches as the threats in cloud and other distributed systems evolve from time to time. Subthemes arising from the analysis of Meng et al. (2013) and Hu et al. (2011) show that changes in strategies, namely the feedback control system and the character frequency-based signature matching, greatly boost the capacity and preparedness of a system to counter new and unknown threats. Such methods permit evolution of security parameters depending on the status of the system, and therefore increase the real effectiveness of security measures. However, the results also show the difficulties of applying adaptive security in large scales, where due to the size of the system, threats may go unnoticed for considerable time. It is therefore recommended that similar studies should be conducted with an aim of enhancing the scalability and applicability of adaptive security architectures to enhance the security of cloud systems.

4.4 Data Encryption Techniques

It is therefore worth to note that data encryption still forms part of the cloud security model where any information that is to be stored or transmitted to be encrypted. The literature review proves that the number of encryption methods is vast; however, the commonly used are symmetric and asymmetric encryption; nevertheless, there is a trend towards using Homomorphic encryption and Quantum resistant. These techniques have advantage of offering security since data can be processed in an encrypted form therefore have minimal chances of being exposed during computation. Nevertheless, the results also bring out the drawbacks of these methods especially in view of their computational costs and structural intricacies. This research indicates that data encryption techniques are ever developing, but current research efforts must focus on advanced research on the efficient application of such encryption in cloud systems where performance is vital.

5. CONCLUSION

This literature review has given an overall synthesis in counter measures against security threats with regard to cloud computing and distributed systems including intrusion detection systems, prevention of DoS attacks, adaptive security systems and encryption of data. This paper has highlighted the need to employ multiple layers of security since different settings present sundry and evolving threats in insecure space. Overall the review shows that the security of cloud and distributed systems has received considerable attention in the recent past and that there are several achievements if albeit that challenges are still apparent particularly with reference to scalability, flexibility, and effectiveness.

With the increase of coverage and utilization of cloud computing in personal and corporate communications and operations, security challenges is set to rise as well. New technologies that are currently being recognized and applied, including artificial intelligence and machine learning, allow us to enhance the corresponding threat detection and prevention. But for these progresses to reach their optimum level, more research needs to be conducted and effective collaboration between fields has to be established. They successfully argued that though, the foundation on which secure cloud computing can be built is in place, continuous work is required to make the structures relevant in the challenging environment in the form of threats.

REFERENCES

[1]. C. Modi et al., “A Survey on Security Issues and Solutions at Different Layers of Cloud Computing,” J. Supercomputing, vol. 63, no. 2, 2013, pp. 561–592.

[2]. J. Hu et al., “Seamless Integration of Dependability and Security Concepts in SOA: A Feedback Control System Based Framework and Taxonomy,” J. Network and Computer Applications, vol. 34, no. 4, 2011, pp. 1150–1159.
[3]. Y. Meng, W. Li, and L.-F. Kwok, “Towards Adaptive Character Frequency-Based Exclusive Signature Matching Scheme and Its Applications in Distributed Intrusion Detection,” Computer Networks, vol. 57, no. 17, 2013, pp. 3630–3640.
[4]. G. Creech and J. Hu, “A Semantic Approach to Host-Based Intrusion Detection Systems Using Contiguous and Discontiguous System Call Patterns,” IEEE Trans. Computers, vol. 63, no. 4, 2014, pp. 807–819.
[5]. Z. Tan et al., “A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis,” IEEE Trans. Parallel and Distributed Systems, vol. 25, no. 2, 2014, pp. 447–456.
[6]. S. Savage, “Internet Outbreaks: Epidemiology and Defenses,” keynote address, Internet Soc. Symp. Network and Distributed System Security (NDSS 05), 2005; http://cseweb.ucsd. edu/~savage/papers/InternetOutbreak.NDSS05 .pdf.
[7]. S. Ram, “Secure Cloud Computing Based on Mutual Intrusion Detection System,” Int’l J. Computer Application, vol. 2, no. 1, 2012, pp. 57–67.
[8]. Mahajan, Lavish, Rizwan Ahmed, Raj Kumar Gupta, Anil Kumar Jakkani, and Sitaram Longani. "DESIGN OF WIRELESS DATA ACQUISITION AND CONTROL SYSTEM USING LEGO TECHNIQUE." International Journal of Advance Research in Engineering, Science & Technology 2, no. 5 (2015): 352-356.
[9]. S.N. Dhage and B. Meshram, “Intrusion Detection System in Cloud Computing Environment,” Int’l J. Cloud Computing, vol. 1, no. 2, 2012, pp. 261–282.
[10]. Racharla, Mr Sathya Prakash, Mr Kontham Sridhar Babu, and Anil Kumar Jakkani. "An Iterative approach for the Restoration of Motion Blurred Images."
[11]. D. Hoplaros, Z. Tari, and I. Khalil, “Data Summarization for Network Traffic Monitoring,” J. Network and Computer Applications, vol. 37, Jan. 2014, pp. 194–205.
[12]. A. Patel et al., “An Intrusion Detection and Prevention System in Cloud Computing: A Systematic Review,” J. Network and Computer Applications, vol. 36, no. 1, 2013, pp. 25–41.
[13]. Srivastava DP. Prof. Anil Kumar Jakkani,“Android Controlled Smart Notice Board using IOT”. International Journal of Pure and Applied Mathematics.;120(6).
[14]. A.K. Jones and R.S. Sielken, Computer System Intrusion Detection: A Survey, tech. report, Dept. of Computer Science, Univ. of Virginia, 2000; http://atlas.cs.virginia.edu/~jones/IDS-research/ Documents/jones-sielken-survey-v11.pdf.
[15]. Agbonyin, Adeola, Premkumar Reddy, and Anil Kumar Jakkani. "UTILIZING INTERNET OF THINGS (IOT), ARTIFICIAL INTELLIGENCE, AND VEHICLE TELEMATICS FOR SUSTAINABLE GROWTH IN SMALL, AND MEDIUM FIRMS (SMES)." (2024).
[16]. Jakkani, Anil Kumar. "Enhancing Urban Sustainability through AI-Driven Energy Efficiency Strategies in Cloud-Enabled Smart Cities." (2024).
[17]. Jakkani, Anil Kumar. "Real-Time Network Traffic Analysis and Anomaly Detection to Enhance Network Security and Performance: Machine Learning Approaches." (2024).
[18]. N. L. Hjort et al., eds. Bayesian Nonparametrics, vol. 28, Cambridge Univ., 2010.
[19]. Srivastava, Pankaj Kumar, and Anil Kumar Jakkani. "FPGA Implementation of Pipelined 8× 8 2-D DCT and IDCT Structure for H. 264 Protocol." 2018 3rd International Conference for Convergence in Technology (I2CT). IEEE, 2018.
[20]. J. Dean and S. Ghemawat, “MapReduce: Simplified Data Processing on Large Clusters,” Comm. ACM, vol. 51, no. 1, 2008, pp. 107–113.
[21]. Nalla, Akash, and Anil Kumar Jakkani. "A Review on Recent Advances in Chatbot Design." integration 3.3 (2023).
[22]. B. Tian et al., “A Mutual-Healing Key Distribution Scheme in Wireless Sensor Networks,” J. Network and Computer Applications, vol. 34, no. 1, 2011, pp. 80–88.
[23]. Srivastava, P. K., and Anil Kumar Jakkani. "Non-linear Modified Energy Detector (NMED) for Random Signals in Gaussian Noise of Cognitive Radio." International Conference on Emerging Trends and Advances in Electrical Engineering and Renewable Energy. Singapore: Springer Nature Singapore, 2020.
[24]. B. Tian et al., “Self-Healing Key Distribution Schemes for Wireless Networks: A Survey,” Computer J., vol. 54, no. 4, 2011, pp. 549–569.
[25]. Jakkani, Anil Kumar, Premkumar Reddy, and Jayesh Jhurani. "Design of a Novel Deep Learning Methodology for IOT Botnet based Attack Detection." International Journal on Recent and Innovation Trends in Computing and Communication Design 11 (2023): 4922-4927.