A ROBUST SECURITY FRAMEWORK FOR CLOUD-BASED LOGISTICS SERVICES

Dr.K.SUDHAKAR[1], KASARLA HARIKAI [2], SNEHA REDDY KOVURI[3], KUCHANA SOUJANYA[4]

ASSOCIATE PROFESSOR[1], UG SCHOLAR [2,3&4]

DEPARTMENT OF ECE, MALLA REDDY ENGINEERING COLLEGE FOR WOMEN (UGC-AUTONOMOUS)
MAISAMMAGUDA, HYDERABAD-500100

ABSTRACT:

In recent years, cloud-based logistics services are quite popular among business enterprises. Cloud computing is attributed to amassed competitiveness by focusing on cost reduction, higher elasticity, flexibility and maximum utilization of resources, which results in successfully achieving business goals. Further, Logistics is the area that requires effective and integrated means of communication, shared risk, collaboration, and orchestration to work successfully and the cloud computing has a lot to offer to this domain. While implementing the cloud-based logistics services, security is considered to be one of the major concerns for corporate entities. This project proposes a robust security framework for cloud-based logistics services. As a result, upon implementation, this model can provide long-term benefits for the business enterprises by improving the overall cloud-based logistics services security.

Keywords: Logistic, Cloud, robust security, security.

INTRODUCTION In recent years, the development of cloud computing has been considered as a unique feature among the key progresses in the area of computing. The distribution of quick, reasonably-priced and scalable services to people and corporate establishments is referred to as cloud computing. It is a ground-breaking standard that expedites the clienteles to implement their project operations and also aides to store the information in the third-party possessed servers. Since the implementation of cloud computing standards has several benefits like pliability, universal availability, convenience, easy maintenance, and economic pay-per-use billing models for corporate entities [1] [2]. The cloud computing services are divided into three major categories, software as a service (SaaS), Platform as a Service (PaaS), and infrastructure as a

service. The applications are running in the cloud are known as SaaS, and it presents an architecture that can run several instances of itself regardless of location. PaaS is a platform that enables developers to write applications to run on the cloud. This would have various applications that can be deployed instantly. The last category is infrastructure as a service that can be accessible by internet technologies and shares the computing infrastructure. The sharing resources are like servers, storage, security, databases, etc. Four different models are suggested in cloud computing. The first model is the public deployment model in which the third parties or any organization operated and distribute services to the public domains. The second is the private model, which is owned and operated by the organization and severed for their internal users. The third model is a community model which operated and organized for specific communities. The last model is a hybrid, which is a mixture of two or more clouds [3][4][5][51][52]. These providers also account for modern-day networks, such as 5G, Internet of Things, as well as novel allocation strategies for handling diversified services [6][7]. Mostly, the Cloud Service Providers are responsible for handling and functioning of the Public cloud infrastructure [51]. Furthermore, it is accessed by an extensive assortment of registered clienteles, and the CSP is liable for the configuration and organization of these services. While considering the private cloud infrastructure, it is handled and functioned by either the CSP or clienteles. However, in some particular scenarios, both the CSP and clienteles are involved in handling and managing the private cloud infrastructure that is owned by a solitary client. The community cloud infrastructure is catered for the needs and utility of a particular selective cluster of establishments. The hybrid cloud is the amalgamation of several disparate cloud models like the public, private and community exemplars for providing tailored infrastructure utilities depending on the needs of an establishment or institution [8][9][10][11]. The organizations can evade a conciliation of their functioning efficacy by implementing the cloud associated infrastructure for swiftly enhancing, successfully recognizing and utilizing the scientific elucidations [12]. Amongst the corporate entities, the private and public cloud associated elucidations are mutually attaining prominence. Nevertheless, as a result of witnessing the goals of the business entities and also considering the cost-to-serve metrics, it can be observed that solely the private cloud models are contending with the predominantly available public cloud models. Additionally, hybrid clouds are designed and tailored based on the specific necessities of corporate organizations. Furthermore, for constructing a hybrid cloud model, at least a solitary public and a

single private cloud infrastructure are essential. Moreover, based on the necessities of corporate enterprises, numerous public and private cloud services can be amalgamated together to build a hybrid cloud infrastructure. Besides, the hybrid cloud services are a seamless and an equilateral blend of both the exterior and interior assets that offer a perfect fusion of swiftness, cost leadership, dynamism and servicelevels [13].

EXISTING SYSTEM:

In the existing system, the details regarding logistics been saved in a cloud so that one can view that anytime. No security to the logistics is provided to logistics as this system is entirely software based.

Drawbacks:

- No security to logistics.
- Purely software based.

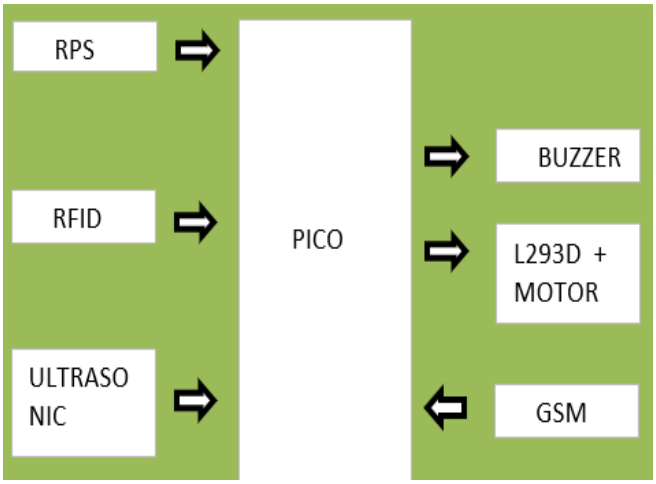
LITERATURE REVIEW

Cloud computing supports various business organizations through high financial savings. The cloud provides streamline processes of the enterprise with adequate productivity and transforming business processes and reducing the cost. The cloud computing helps in business to attain scalability, more satisfied customers and provide reliable backups. In the era of cloud computing, various researches have been conducted to enhance the facilities of cloud-driven networks. Uchenna et al. [31] gave a cloudbased virtual organization framework that Integrates Cloud Computing Model (CCM) with the Virtual Value Creation (VVC) framework of Virtual Organization (VO) to improve traditional methods of business. Mushtaq et al. [32] focused on information security in cloud computing. The authors focused on secure data transmission, encryption of data and it is Processing, Secure database, Shell, and logs in the clouds. Ukil et al. [33] give a security framework to manage the cloud system more efficiently and provide security and mitigate threats. Tawalbeh et al. [34] suggested cloud computing framework in which the data is classified based on the importance and important data is encrypted. Arjunan and Modi [35] suggested an intrusion detection system for clouds based on signature and anomaly-based techniques. The IDS helps to identify various attacks in the cloud. Marwan et al. [36] suggested a

secure framework for cloudbased medical image storage in which segmentation and watermarking mechanisms are used to provide privacy in the saving of a medical image. Al-Bahadili et al. [37] suggested Cloud Collaborative Commerce (cc-commerce) model to Supports cost-effective computing resources for businesses and reduce installation and running costs, delay, Security, etc. Tawalbeh et al. [38] presented the secure mobile cloud computing framework which used trust delegation technique to provide better security and performance. The state-of-the-art comparison of existing approach for cloud-driven networks is presented in Table 1. Some other research works to follow are, cloud computing governance [39], securing the cloud-Governance[40, big data fraud detection[41], single sign-on for clouds[42], proactive user-centric security[43], preventing insider cyber threats[44], authentication and authorizations[45], email spam prevention in logistics[46], proxy network formations[47], firewall management[48][49]and big-traffic evaluations [50].

PROPOSED SYSTEM:

In the proposed system, we have used the hardware interface in order to provide security and safety to the logistics. For intruder detection, an IR sensor is used; for fire detection, a fire sensor is used. If any of these conditions becomes true, the camera will capture the image and will send it to the authorized person.



Advantages:

- Security to logistics

- Immediate alert when a fire accident occurs or intruder comes.
- Hardware interface makes it more efficient to use.

Applications:

- In Industries like automation, manufacturing to provide security and safety for logistics.

CONCLUSION Cloud-based logistics management helps business organizations to support flexible and reliable handling of a large amount of data. The article discussed unmentioned and undiscovered security issues that positively affect cloud systems. Recently, a wide range of researchers emphasized the known problems of the cloud systems and suggest various solutions. However, if a cloud system is to be widely adopted, better solutions are still needed. In this article, a conceptualized robust security framework for cloud-based logistics services is presented. Moreover, a security enhancement layer is included at each layer of the cloud with a feasibility study on protecting user information in the logistics services ambiance. Also, the Data Residency for cloud-based logistics services is elaborated with Data Security analysis. Further, the article discusses the possible solutions to handle the security concerns of the logistic model. In the future, the cloud-based security through misbehavior detections and vulnerabilities assessment will be focused.

REFERENCES

1. Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A., (2011). Cloud computing: The business perspective. Decision support systems, 51(1), pp.176-189.

2. Xu, X., (2012). From cloud computing to cloud manufacturing. Robotics and computer-integrated manufacturing, 28(1), pp.75-86.

3. Singh, A., Mishra, N., Ali, S.I., Shukla, N., and Shankar, R., (2015). Cloud computing technology: reducing carbon footprint in beef supply chain. International Journal of Production Economics, 164, pp.462-471.

4. Joosen, W., Lagaisse, B., Truyen, E. and Handekyn, K., (2012). Towards application driven security dashboards in future middleware. Journal of Internet Services and Applications, 3(1), pp.107-115.

5. http://www.manufacturing.net/articles/2012/03/the-rise-of-cloudcomputing-extends-to-plm [Accessed 18 Jun. 2016]. 6. Sharma V, Srinivasan K, Jayakody DN, Rana O, Kumar R. Managing Service-Heterogeneity using Osmotic Computing. arXiv preprint arXiv:1704.04213. 2017 Apr 13.

7. Sharma V, YouI, Jayakody DN, Atiquzzaman M. Cooperative trust relaying and privacy preservation via edge-crowdsourcing in social Internet of Things. Future Generation Computer Systems. https://doi.org/10.1016/j.future.2017.12.039, 2017 Dec 28.

8. Cloud Computing Competence Center for Security, (2015). What are Deployment Models in Cloud Computing? [online] Available at: http://www.cloud-competence-center.com/understanding/cloudcomputingdeployment- models/ [Accessed 18 Jun. 2016].

9. Rochwerger, B., Breitgand, D., Levy, E., Galis, A., Nagin, K., Llorente, I.M., Montero, R., Wolfsthal, Y., Elmroth, E., Caceres, J. and Ben-Yehuda, M., (2009). The reservoir model and architecture for open federated cloud computing. IBM Journal of Research and Development, 53(4), pp.4-1.

10. Sultan, N., (2010). Cloud computing for education: A new dawn?. International Journal of Information Management, 30(2), pp.109-116.