International Journal of Education and Science Research Review
E-ISSN 2348-6457
Volume-2, Issue-4 July-August- 2015 P-ISSN 2349-1817
www.ijesrr.org Email- editor@ijesrr.org

SCALABLE AND SECURE CLOUD FRAMEWORKS FOR ENHANCING PERFORMANCE IN NEXT-GENERATION INTERNET APPLICATIONS

M E Purushoththaman, Research Scholar, Sunrise university, Alwar

Dr. R. K. Pandey, Professor, Sunrise university, Alwar

ABSTRACT

Our proposed catalog is an organized list of all the new features added to the classic Internet of Things. This article provides a high-level overview of the Internet of Things (IoT) from the vantage points of the fields of data science, networking, big data, and connecting technologies. In addition, we provide a general model for cloud computing security that may assist meet cloud security and privacy needs while also protecting them from different types of threats.

Keywords: Energy, big data, data science, network**,** IoT.

INTRODUCTION

"Things" that are physically present and equipped with sensors, software, and other technologies form what is known as the "Internet of Things" (IoT). This network allows these "things" to connect to one another and share data over the internet. In addition to the relay idea and the use of AI in future generation networks, the Internet of Things is now being used in every industry, including agriculture, energy, finance, healthcare, manufacturing, transportation, and so on. For example, if a server and a computer are located on opposite sides of the room, they may still interact with each other over a relay network. So, data must be "relay"ed" from one device in the network to another, called a node, before reaching its final destination. An example of a relay network that is well recognized is the Internet. A user might be seeing a web page hosted on a server in another country thanks to data sent and received via a network of interconnected nodes. Through the use of computers and other technological devices, artificial intelligence attempts to simulate human intelligence in order to solve problems and make decisions. There is an art and a science to creating intelligent robots, particularly proficient computer programmers. Artificial intelligence (AI) is not limited to physically observable actions, even if it is a comparable problem to use computers to study human cognition.

Resolving concerns about data privacy and security during cloud implementation is the industry's top priority. The International Data Corporation (IDC) ranked the difficulties associated with cloud computing in a 2009 August poll. According to the survey's findings, cloud computing security is the main issue. The multi-tenancy feature of cloud computing, together with the practice of outsourcing important applications, infrastructure, and sensitive data, is the major cause of cloud computing's security and privacy issues. A lot of people and businesses are worried about how the new cloud system will handle privacy and security.

LITERATURE REVIEW

Cloud computing is a big technology that can help companies of any size, says Harshit Srivastava et al. (2015). Nevertheless, there is an urgent need to address the serious anxiety around adoption caused by security and privacy issues. Concerns about data confidentiality arise among consumers in the presence of a comprehensive taxonomy of cloud-based attacks. Security issues may be classified according to data,

availability, compliance, user role, and vendor role. Data centers, policies, reasoning, and cloud technologies are only a few examples of the methodological and technical challenges that could compromise security. Other potential threats include locations, laws, and other physical aspects. Their research looks at a number of attacks and security breaches that occurred in data centers. Some examples include a huge storm in North Virginia in June 2012 that affected Amazon's Data Center, a malfunction in March 2011 at Google that nobody saw coming, and so on. Physical, environmental, and virtualized security are all the vendor's responsibilities, according to this study's authors, who reviewed many survey data sets.

Cloud computing, according to Shipra Dubey et al. (2014), is a novel concept that, despite serious security concerns, provides on-demand access to scalable and virtualized hardware, software, and bandwidth via a web browser or service. The main topics covered in this article include online security threats and attacks, browser security, malware injection attacks, XML signature element wrapping, and IDS/IPS point-to-point encryption and XML encryption as solutions.

Shikha et al. (2014), claim that attackers now have more opportunities to conduct different types of attacks due to the rise of cloud computing. This is now their number one concern; therefore they are taking extra precautions to protect the cloud and all of its services. The study covers a wide range of topics, including denial-of-service attacks (attacks on firewalls, intrusion detection systems, black holes, and sink holes), malware injection attacks (on file allocation tables, operating systems, and cross-checking), side-channel attacks (on virtual firewall appliances, on randomly encrypted and decrypted data), and authentication attacks (on site keys, virtual keyboards, and shared secret questions). The authors also came to the conclusion that, as their study progressed, they would keep collecting cloud vulnerabilities and attacks to show how well the attack worked.

A FRAMEWORK FOR SECURE CLOUDS

Every one of its three main security features presents unique threats to users' personal information and data stored in the cloud. The parts in question are:

Determines what the cloud's security and privacy needs are in terms of things like authentication, authorization, integrity, and more. Dangers and assaults: alerts on various dangers and assaults that clouds are susceptible to. Pay close attention to the worries and dangers associated with cloud computing. In the parts that follow, we'll go over each rule specifically.

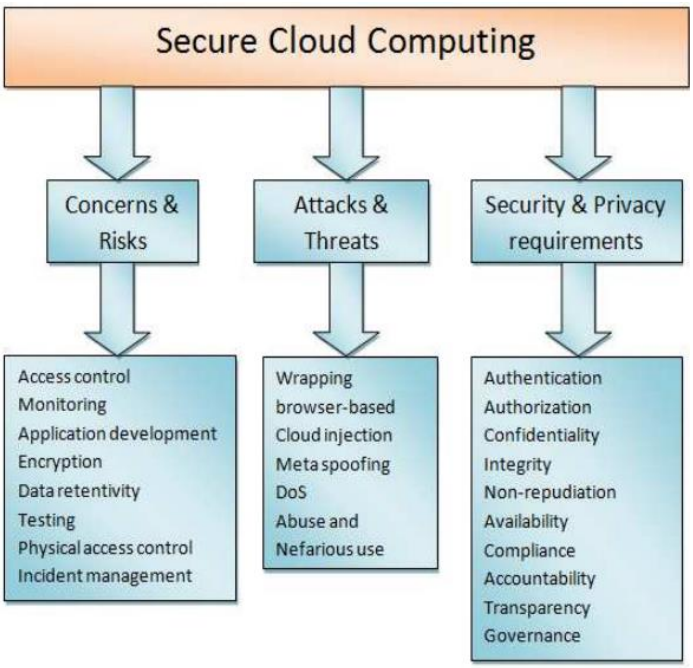

Fig. 1: A Framework for Secure Cloud Computing

Next-Generation Advancements in the Internet of Things (IoT) Technologies

Here we outline the fields of data science, network science, and big data before going on to talk about the latest developments in this field. We propose improvements to the Internet of Things (IoT) for the future by investigating several linking technologies, including machine learning, artificial intelligence, and federated learning. We also go over the pros and cons, as well as the most current research that is pertinent to the topic.
"Big Data"

Here, we fill readers in on what big data is, the benefits it offers, the five Vs, and the most current trends in its expansion. End devices in the IoT produce massive amounts of data when sent across the network. Expertise in statistical techniques and programming is necessary for collecting, analyzing, and managing massive datasets [36]. End devices connected to the Internet of Things (IoT) create the data. Step two involves gathering relevant data, and step three involves analyzing it. Over time, the performance of the end devices that make up the Internet of Things (IoT) decreases due to the generation of various kinds of redundant and noisy data over networks. Reducing inaccuracy of risk and providing correct data is the main benefit of big data [36]. The five Vs, a name for the five distinct dimensions provided by big data. The magnitude of big data is represented by the volume in this graphic. The data are often classified as big data or not, mostly based on their volume. Data growth dynamics and prediction patterns are shown in a recent study [37]. Unstructured, semi-structured, and structured data are all examples of the types of data that fall under the umbrella word "verity" when discussing data created by people or robots. The "veracity" of data is defined as its precision, trustworthiness, authenticity, and excellence. Due to the many origins of the data, it is essential that we verify it before processing. Value rounds out big data technologies. Data value is defined as the extent to which data aid in decision-making. So, it's important to use the right data analytics to get the most out of large data.

Figure 2. Five Vs of big data.

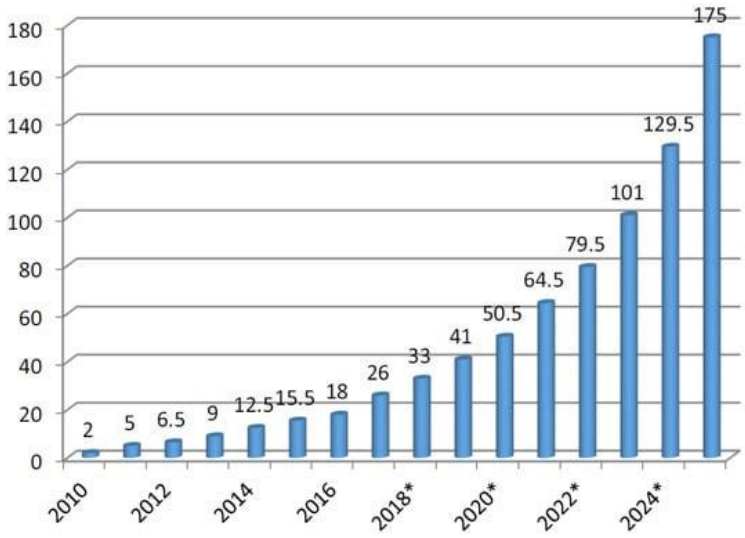

Figure 3. Data growth prediction dynamics worldwide.

Recent Advances in Big Data

Here, we lay out the most current state-of-the-art research and the comprehensive perspective of the Internet of Things. all things considered, including the interconnections between IoT endpoints and big data. Internet of Things (IoT) endpoints are linked over the cloud. This includes CCTV cameras, smart home gadgets, and smart traffic light sensors. Big data refers to the massive amounts of data carried by these gadgets. The data is presented in many forms. The first step is to save the data on an inexpensive storage medium. Technology in the cloud powers the storage. Big data analytics were used to collect this data, and the five Vs were used to carry out the big data operations. Large storage devices, like clouds, etc., have this data saved. Data analysis utilizing technologies like Spark, Mapreduce, Skytree, etc., is the final phase. The analysis of data is done by these instruments. The employment of intelligent software and the Internet of Things caused a problem during data collecting. Both pre-processing and meta-data generation are methods of intelligent data pre-processing. Data is sent from the Internet of Things end devices to various processing centers. Due to its massive scale, the data must be sent rapidly to various processing centers. Data loss of significant value could occur in the event of any lag. For example, this model is very intelligent and has great computational efficiency; many researchers worked toward this

goal. Specifically, they found that deep learning bolsters real-time apps. The benefits are many. Energy efficiency and spectrum use in the Internet of Things are two areas where it contributes. The authors of this paper proposed using the singular-value decomposition (SVD)-QR method for large-scale data pre-processing in deep learning.

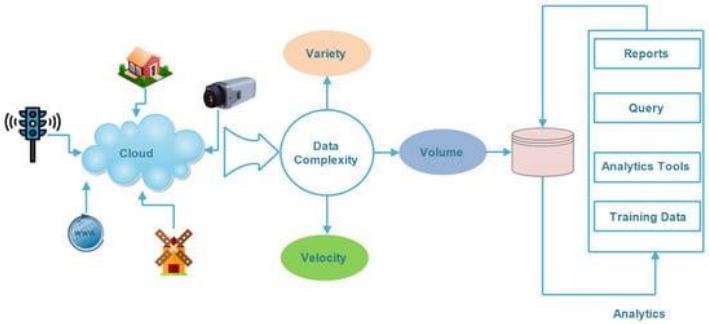

Figure 4. A holistic view of the IoT and big data analytics.

Data Science

This section begins with an overview of data science as a field, followed by a discussion of its recent developments and their benefits. The Internet of Things (IoT) has altered the character of modern business as well as everyday living. It has linked companies and consumers into overlapping organizations and transformed humans into smart gadgets. Data science incorporates ideas from many other academic disciplines, including distributed computing, data mining, and machine learning. This statistic clearly shows that this area of study has applicability in many different fields. Data science is a useful tool for processing and obtaining useful information. Data cleansing, data exploration, data mining, and the other six iterative processes form the basis of the lifecycle. In order to achieve business goals, the data science lifecycle is useful for generating insights and making predictions utilizing analytical and machine learning techniques.

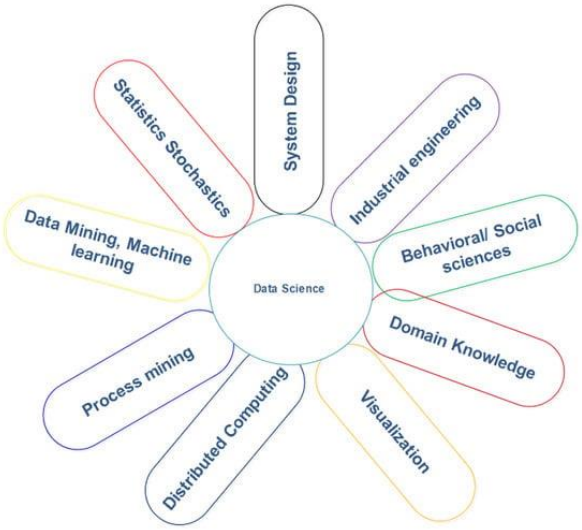

Figure 5. Data science.

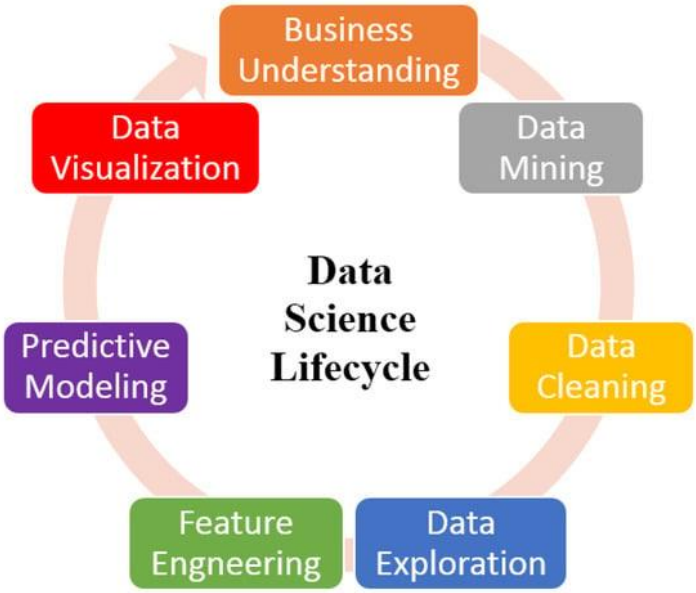

Figure 6. Data science lifecycle.

The Networking Tools

Key linking technologies, such as AI and ML, are highlighted here along with their usefulness and benefits. Thus, cyber-physical systems (CPSs) are formed by interconnected smart items over the Internet. The question that emerges is how to deal with a deluge of produced data while reducing computing power requirements [64]. Data scientists and AI researchers are eager to find the solution to this issue. By boosting the intelligence of learning facilities via smart objects, ML in the IoT aims to bring about full automation. As an example, a fire alarm may be set up to warn people of impending danger in a commercial or residential kitchen. The use of ML techniques in conjunction with the incorporation of IoT applications makes this a reality. For example, a novel and effective approach to MIoT security has been suggested, which integrates ML with big data processing.

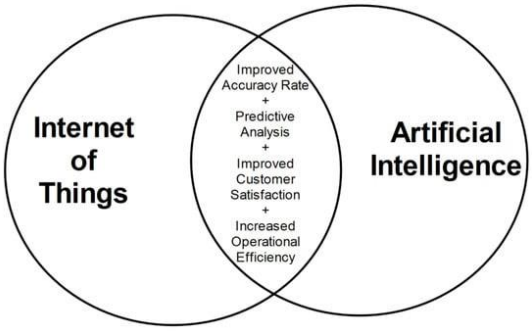

Figure 7. The common functionality in the IoT and artificial intelligence.

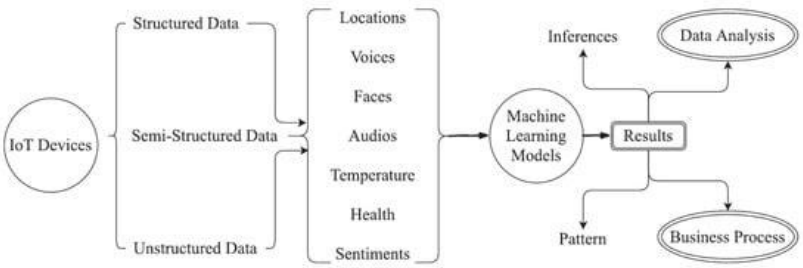

Figure 8. The basic machine learning-based model integration with the IoT.

IOT For Data Management, Security, Privacy, And Compliance

As the number of end devices linked to the Internet of Things (IoT) grows, data security becomes an increasingly pressing issue. Users and stakeholders are essential parts of the Internet of Things (IoT). Their critical data is expected to be secure and kept private. Limiting user privacy involves exposing the end devices of the Internet of Things. Companies should be cautious not to let sensitive information slip through the cracks. Data science techniques have emerged as a key component in user security in recent years. Two primary characteristics, authenticity and integrity, are involved in the security of Internet of Things applications. Two crucial requirements must be satisfied in order to provide the security feature in the IoT: firstly, appropriate authentication, and secondly, device identification. There is no governing body for the IoT devices, and they come from a wide variety of manufacturers. All of these things come together to form the conventional business, which relies on system management. Current global priorities are on expanding research into cutting-edge techniques for detecting operational Internet of Things (IoT) devices, particularly in decentralized or distributed networks. Researchers need to find new IoT frameworks since old ones don't operate with IoT systems anymore because of limitations like memory and battery life.

Using cutting-edge technologies like ML, AI, blockchain, etc., to beef up security is another consideration. Integrating ML methods with the IoT makes it possible to analyze massive amounts of data. Raising the rates of precision and operational efficacy would be beneficial. Both supervised and unsupervised learning are components of ML approaches. Machine learning solves security problems including detecting intrusions, anomalies, malware, impersonating someone, injecting fake data, identifying illegal IoT devices, etc. A key point raised by the writers was the incorporation of AI into the IoT. The Internet of Things (IoT) with artificial intelligence (AI) capabilities may boost operational efficiency and accuracy in predictive analysis. In addition to facilitating permission, protecting privacy, detecting viruses, etc., AI also offers a degree of security. Identity verification, trust management, safe computation and storage, data integrity and secure communication, access control, information sharing, firmware detection, self-healing, and many more issues may be addressed using blockchain technology. Fl is the name of another prominent technology. Ideal for Internet of Things devices that never run out of resources. Both data security and scalability are enhanced.

Scalability and Unified Messaging

As a rule, message passing in IoT systems makes use of hybrid approaches. Whether it is decentralized or centralized may be situation dependent. A sensor that communicates with the cloud (S2C), a sensor that communicates with the edge (S2E), and an edge to cloud (E2C) are all components of the message communication. For real-time applications, these centralized modes like S2C aren't up to the task. Furthermore, existing protocols, like Azure IoT, which are cloud-based, fall short of the quality-of-service standards needed by IoT devices. The necessity to include the cloud and edge layers into new communication protocols is therefore imperative. Internet of Things (IoT) data scalability is crucial. Organizations should improve their methods for recording big data as, on average, IoT end devices produce large data on a second-by-second basis. To resolve this, it is necessary to use new models and communication protocols for the Internet of Things (IoT) cloud and edge layers.

Network Programming for Internet of Things Application Support

An up-to-date approach, software-defined networking (SDN) lets administrators set up, administer, and control the OSI model's networking components. Problems with conventional networks' static design inspired the development of software-defined networking (SDN). Recently, SDN has shown promise in a number of areas, including optimization of flows, bandwidth allocation, and more. Using the Internet of

Things to explore it has never been done, unfortunately. Therefore, conventional SDN protocols should be the primary focus of the research.

Storage and Collection of Big Data

Data visualization, analysis, and processing are complex and difficult processes. It is possible that the findings will be less efficient if we do the analysis in a certain manner. Due diligence in mastering the IoT sector is, hence, essential. The format and structure of the data obtained by the sensors may be determined with its aid. Garbage data will be the outcome if our expertise is limited. The total cost will rise as a result of this. Internet of Things (IoT) large data presents unique challenges related to the five Vs.

Differential and Technical

The end devices that make up the Internet of Things (IoT) may take several forms, connect over a variety of protocols, and exchange data in a wide variety of ways. As a result, the Internet of Things system has to provide each device a distinct ID in order to offer security and verification.

Proposed Security Model

We have developed a general cloud computing security model based on the aforementioned architecture. This model helps meet the security and privacy needs of clouds while also protecting them from different vulnerabilities. Figure displays the model together with the following security units:

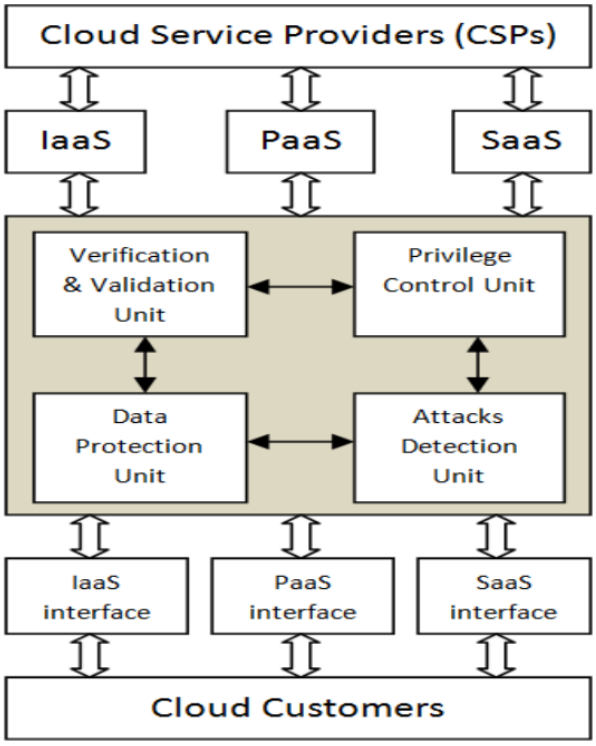

Figure 9: Cloud Computing Security Model

Section for Validation and Verification (V&V)

To guarantee the accuracy of data and services stored in the cloud and to authenticate users, this unit is essential in cloud computing. Because the cloud computing environment is accessible by both customers and providers, this security component is crucial because it allows for the usage or provision of many

services and applications. It is the responsibility of CSPs to demonstrate to consumers, using means such as suitable signature algorithms, that the data and services they are accessing are authentic. This kind of digital signature will allow users to confirm the legitimacy of the data and services that are made accessible to them. This safety feature may also use two-factor authentication and one-time passwords (OTP).

Control Unit for Privileges

In order to regulate how various entities use the cloud, this security unit is essential. It uses a set of laws and regulations that regulate who may do what in the cloud to safeguard users' privacy and guarantee the integrity and secrecy of data. Based on their account type, users in the cloud are assigned varying degrees of access rights and resource ownership. By using an identity-based decryption technique, only authorized users will be able to access the encrypted data. Take healthcare cloud computing as an example. Different practitioners may have different levels of access to patients' data, depending on their level of involvement or specialization in treatment. Patients also have the option to allow or deny sharing their information with other healthcare practitioners or hospitals. This part may use encryption and decryption methods like AES and RC4 to make sure data stays private.

Information Security Group

For instance, electronic health records (EHR) kept in the cloud may include individuals' personal information and medical history; this data can be very sensitive and important. Important financial data (such as customers' account numbers, balances, and transactions) or sensitive national security documents may also be stored by these. These files should be safe from harm thanks to the secure servers provided by a cloud security paradigm. Data removal and retrieval from the cloud should also be secured by these servers. Since cloud users are unaware of the physical location of their data, it is crucial to secure both the storage and processing of their data. Data protection techniques including obfuscation, truncation, redaction, and others may be used in this security component. Data security may also make use of encryption methods. It is possible to use Message Authentication Code (MAC) and hash functions in this unit to ensure valid data.

Detection and Prevention of Attacks Unit

Data and the cloud's physical and virtual computing resources are at risk from a wide variety of assaults and malicious activities. Attacks may take many forms, but generally refer to any coordinated effort to compromise the cloud's essential security features (such as availability, confidentiality, or integrity). In order to safeguard cloud resources from different kinds of abnormalities, the cloud security system should include components that can detect and prevent attacks. For instance, in order to ensure the greatest availability of vital commercial, government, health, and other service information, denial-of-service assaults should be minimized to a minimum. High availability solutions, such active/active clustering and dynamic server load balancing, may help with this. Additionally, you may use tried-and-true methods for preventing Distributed Denial of Service (DDoS) attacks, such synchronous cookies and connection restriction. Protecting cloud resources from hackers, viruses, and malware should be a top priority for the next generation of IDS/IPS firewalls.

CONCLUSION

This study presents a literature analysis on cloud computing security issues and proposes a methodology to catalog cloud deployment-related security and privacy needs, attacks, threats, concerns, and dangers. Using this as a starting point, we developed a general model for cloud security that can shield clouds from different threats while still meeting users' needs for privacy and security. We think cloud providers and enterprises should do more to provide a secure, reliable, and protected cloud computing environment.

REFERENCES

1. H. Srivastava and S. A. Kumar, "Control Framework for Secure Cloud Computing," J. Inf. Secur., vol. 06, no. 01, 2015.

2. M. Sulochana and O. Dubey, "Preserving data confidentiality using multi-cloud architecture," in Procedia Computer Science, 2015.

3. B. Sumitra, C. R. Pethuru, and M. Misbahuddin, "A Survey of Cloud Authentication Attacks and Solution Approaches," Int. J. Innov. Res. Comput. Commun. Eng., 2014.

4. Jacek Góra, Góra "QoS-aware resource management for LTE-Advanced relay-enhanced network" Year of conference 2014, Góra EURASIP Journal on Wireless Communications and Networking 2014, 2014:178 http://jwcn.eurasipjournals.com/content/2014/1/178 @ springer

5. Byungkwan Kim and Taejoon Kim, "Relay Positioning for Load-Balancing and Throughput Enhancement in Dual-Hop Relay Networks", year of conference 2021, DIO: 10.3390/s21051914

6. Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems, 25*(6), 599–616. https://doi.org/10.1016/j.future.2008.12.001

7. Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W. (2010). Toward secure and dependable storage services in cloud computing. *IEEE Transactions on Services Computing, 5*(2), 220–232. https://doi.org/10.1109/TSC.2011.24

8. Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2013). A survey of mobile cloud computing: Architecture, applications, and approaches. *Wireless Communications and Mobile Computing, 13*(18), 1587–1611. https://doi.org/10.1002/wcm.1203

9. Zhou, Z., & Buyya, R. (2014). Augmentation techniques for mobile cloud computing: A taxonomy, survey, and future directions. *ACM Computing Surveys, 47*(2), 1–33. https://doi.org/10.1145/2656204

10. Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. *IEEE Internet Computing, 16*(1), 69–73. https://doi.org/10.1109/MIC.2012.14