International Journal For Technological Research In Engineering
Volume 10, Issue 9, May-2023 *ISSN (Online): 2347 - 4718*

ENHANCING THE DATA INTEGRITY IN SERVERLESS GREEN CLOUD COMPUTING & IOT NETWORKS

Aishwarya Shekhar
Research Scholar,SCSE
Galgotias University
Greater Noida, India

Abstract—Green Cloud computing controls the entire information technology (IT) by allowing omnipresent access to a distributed pool of configurable device tools and a higher degree of limited managed services. The allocation of resources and the cost effectiveness of these resources is a prerequisite for this process. In today's scenario, building green cloud architecture is easily reliant based on the availability of high capability networks, low-cost computers, storage devices like hardware virtualization with a service-driven architecture and self-employed utilities. Internet of thing is a new technique through which the devices are connected through each other with the help of internet. In the context of IoT, confidentiality caters for protecting privacy of IoT devices integrity looks after the data contained within the device while availability covers accessibility of the device. This article will focus on the aspects of maintaining data integrity.

Keywords—Green Cloud Computing, Cloud Computing, Server less, Internet of Thing, Networks

1. INTRODUCTION

Green computing is good for our environment it is also referred to as green technology, but if consumers stop for a second and count how many times a day we are not using or leave behind our devices on things such as tablets, laptops or even a desktop, we would be impressed. The importance behind this is not only about saving energy, but also thinking about the many risks there are by leaving devices with free access to personal information. The goal of green computing is to attain is to attain economic viability and improve the way computing devices are used. Green computing practices include the development of environmentally sustainable production practices, energy efficient computers and improved disposal and recycling procedures [1]. There are other goals of green information technology, most notably at the design and manufacturing stages. The Internet of Things (IoT) is promising to open up many new opportunities for businesses to offer new and exciting services. However, with the myriad of devices and business assets connected open to the internet, the need for a strict and reliable approach to security is essential. When we think about data of an IoT device we should think about not only the data being generated or used by it but also its own programming data, this including all aspects of program software, configuration parameters and operating system software. To guide the process of integrity it is helpful to consider three different states that data can exist, namely in motion, at rest and in process [2]. Any breach of data integrity will mean that an IoT device cannot operate correctly but it also potentially exposes the device to being exploited and become a compromised platform from which other attacks can be launched. The usual method of verifying the integrity of data is by a mathematical algorithm called a hash, of which the secure hash algorithms (SHA) is most popular.

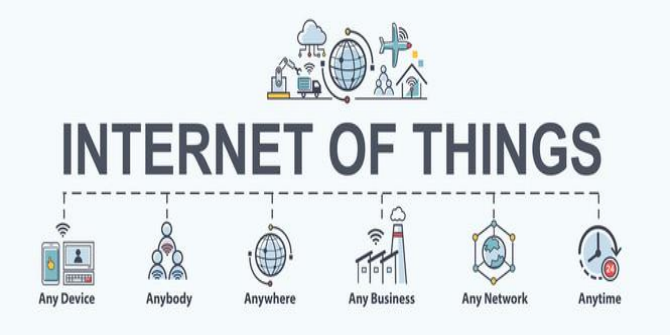

Fig 1. Internet of Things

II. BACKGROUND

The Services-Oriented Architecture (SOA) has been a key discipline for addressing the difference between IT and business services. In recent decades, companies have created SOA and distributed networks that cover numerous business areas, including letters of mail, logistics, financing and banking [3]. The key of SOA is to produce standardized communication protocols for individual, self-describing software modules, all of which are usable and accessible through the network. Web services technology has incorporated this idea as a significant implementation in the construction of new web applications. For years, web applications built on three-tier architecture have been created, which views an application as three separate layers – presentation, corporate logic and data. The architecture essentially specifies how problems are separated between frontend, data and backend[4]. The principle of decoupling helps developers, without affecting other levels, to make major layer changes and thereby easily maintainable applications. In the meantime, business logic and data layers can be introduced as web servers from the viewpoint of SOA architecture, allowing connectivity using common protocols based on the Internet. Web services have recently published

APIs to teach users how to communicate and share data. A webservice that runs on a physical or virtual machine, is installed and supported by a database server. The web server supports HTTP data transmission, which listens to and returns HTTP queries and replies, as well as HTTP requests. There are specifications for setup and servicing when they are hosted on a physical or virtual machine. In order for a computer to be able to run the web service, a development team has to review and determine machine requirements (such as processing power, memory and storage spaces). The phase involves the acquisition of hardware and software licenses as well as time and team commitment to set-up whether the server is installed in-house. Such a web server demands routine servicing, such as error detection, rational emergency management planning and updating (the server is either over-loaded or crashed), which requires human resources (both software and hardware components). Web systems will, on the other hand, be implemented on a computer network, where cloud providers have the infrastructure and computer tools needed to host and execute applications [5]. When this method is used, the team discards questions about hardware modules, but the work of configuring the server and operating system is still persistent and requires human efforts. Cloud providers recently launched serverless computing systems, also called the Function as a Service (FaaS). For instance, Amazon's computer services, Amazon Web Services (AWS) Lambda, provide the container of an ephemeral feature for the execution of the code of the application. The container is an environment fully configured to work with such source code. The team will then focus on writing back end codes for corporate logic and installing them on networks without regard to the infrastructure sophistication and maintenance.

Fig 2. Data Integrity

III. ATTRACTIVENESS OF SERVELESS GREEN COMPUTING

Serverless service helps market expansion by making it easier to program the cloud, which attracts more users and improves current customers' use of cloud technologies. Latest studies have found, for example, that about 24% of serverless users are new to cloud computers, while 30% have serverless computing used by current cloud clients. Furthermore, the short-term, limited memory and statelessness of cloud services enhance computational multiplexing by facilitating unused tools for these activities [6]. Cloud providers may also use machines that are less common because the instance form is accessible by cloud providers — for example, older servers that are less appealing to server cloud users. Both advantages boost revenue from available services. Customers benefit from greater productivity in programming, and cost efficiency can also be achieved in many cases when the underlying servers are used more often. While serverless computing makes it easier for consumers to do so, Jevons paradoxically implies it would boost cloud usage instead of reducing it as greater reliability increases demand by adding users. Database consumers prefer serverless computing, as novices can implement features without any cloud architecture awareness, and since professionals can save time for implementation and work on application-specific issues. Serverless consumers can save money because functions are performed only when incidents arise and fine-grained accounting (usually 100 milliseconds today) ensures that they only pay for what you use according to what they book. Investigators have been drawn to server-less and cloud functions in particular, as it is a modern abstraction of calculation for the general purpose that aims to become the future of cloud computing and as there are numerous possibilities for enhancing existing efficiency and addressing its current limitations[7].

IV. SECURITY ISSUES IN SERVERLESS GREEN COMPUTING

1. Security and Privacy: Data security for any company which is still subject to inspection, is a fundamental part of this. Because of security concerns, companies are hesitant to purchase insurance from the providers. In competition with rapidly moving technologies, they risk losing consumer data and their secrecy is high. The real storage, which adds to the security issues of the companies, is also not revealed. This confidential information is protected by traditional firewalls through data centers (owned by companies).Service providers in the cloud model ensures the safety of data on which companies can rely blindly on them.

2. Data recovery and availability: Service level arrangements are strictly adhered in all enterprise applications. Operational teams play an important role in service level agreement administration and program runtime governance. Below are some of the activities carried out in the manufacturing area by the technical staff.

3. Lack of standards: Cloud platforms have documented the interfaces, because of the requirements of these interfaces are not limited, the cloud is typically interoperable. The Open Grid Forum develops the Open Cloud Computing Interface to address this problem and the Open Cloud Consortium works on the principles and policies of cloud computing with ideas from different angles. The results of such groups demand further guidelines, but it is not certain if the services are designed to meet people's requirements by the deployment of suitable interfaces. But staying up to date with the new developments will increase the value of the results [8].

4. Interoperability: Software applications should be able to

use other platform services. This is possible through web services. However, it is very complex to develop such web services.

5. Computing performance: In order to deliver cloud-intensive computer services, high network capacity is needed, which means greater costs. When achieved with a lower bandwidth, it does not fulfil the required performance of an application.

6. Portability: This is another problem in the cloud world that allows programs to move from one cloud vendor to the another. Vendor lock-in problems should not be present. Since, the usage of many common languages that cloud services use on websites, this has not yet been made possible.

7. Destruction of Data: When no further data is required, the data must be entirely deleted. Because of physical storage characteristics, the lost data is still available and may be restored or retrieved. This obviously results in classified data being disclosed to unauthorized cloud parties.

8. Group Key Agreement: Multiple network nodes participating in a common group, sharing a common cryptographic key. This is an area of active research as restrictions on both computational complexity and network utilization are frequently imposed. It must be enforced that perfect backward and forward key secrecy be maintained to prevent any decryption of any messages received while not a member of the group.

9. Confidentiality: It is computationally infeasible for the intruder to determine the message other than the receiver. This can be achieved through the use of cryptography. The main goal of cryptography is to keep data scheme and utmost privacy of the data. In two-party communications a series of options exist. For symmetric cipher systems, a shared common key is fed into an encryption scheme. This key is agreed upon using a key agreement protocol, much like Diffie-Hellman. For asymmetric cipher systems, a set of keypairs must exist and be known. A sender would then encrypt a message with the receiver's public key, and the receiver would then decrypt with their private key. This requires no key agreement, but does require an up-to-date key database that must be known and trusted to be secure and safe from tampering. In multi-party communications, as in collaborative broadcast-based groups, encryption serves as a membership border. By the nature of broadcast, all nodes within a sender's broadcast range receive the message, but with encryption, only those nodes with knowledge of the encryption key will be able to understand the contents [9].

10 Integrity Verification: Knowing and being guaranteed that a received message has not been tampered with or altered in any way. This is generally done with the employment of hashing. A message of n length is represented by a constant length bit string of k bits. Any change in the message results in a dramatically different hashcode, and any alteration of the hash will clearly not match the data. Using just hash code values does not prevent a third party from modifying the payload and injecting a new and valid code[10].

11. Authentication: Knowing and being guaranteed that a received message from sender "S" was in fact sent by 'S'. This functionality is combined with integrity verification, and provided through the use of digital signatures, and, in a more connected world, supported by digital certificates and the Public Key Infrastructure (PKI). Signatures are based on public and private key pairs. A message would be signed with the sender's private key, and later verified with the sender's public key. This provides proof a particular sender sent any given message. Signing includes a mixture of private key and a hash of the message. This verification may be done by any party privacy to the signature and the signer's public key[11].

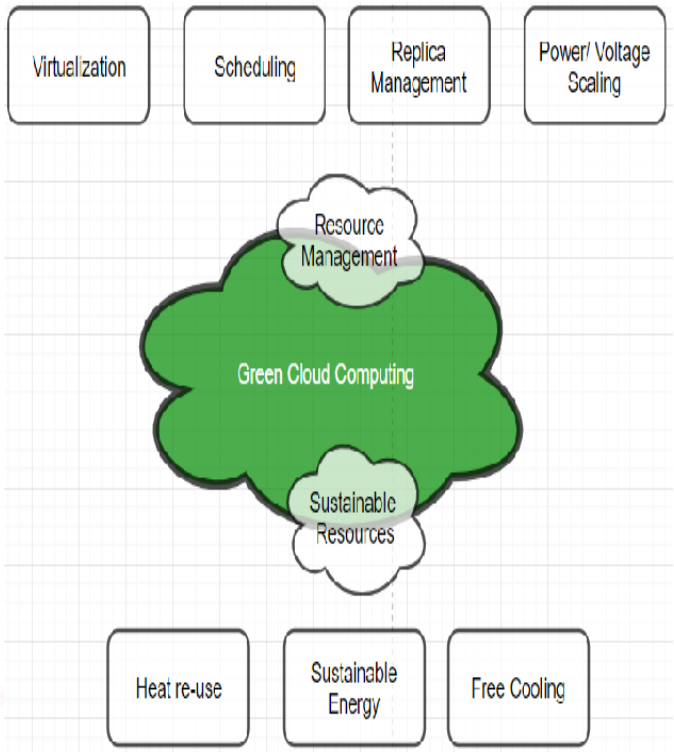

Fig. 3 Green Cloud Computing

V. TYPES OF DATA INTEGRITY

Physical: Applies to hard copies and digital files, especially in a disaster (e.g., flooding, fire, power outages), as related to the safeguarding of data during storage and retrieval.

Entity: Focused on the characteristics of the tables that are used to store and connect data in relational databases.

Domain: In a database, refers to the suitable values that a column may contain (e.g., constraints on format or the amount of data entered).

Referential: A set of procedures for how data should be stored and used to ensure consistency and accuracy and prevent duplication, or prohibit the entry of data that does not apply [12].

User-defined: Rules and restrictions created by a user to meet

their specific requirements

Logical: Protects data while in use in relational databases

VI. DATA INTEGRITY IN IOT NETWORKS

Data integrity and reliability problems threaten to defeat the purpose of using intelligent and connected IoT networks. Therefore, employing the right tools and measures is imperative for maintaining data integrity in IoT networks. IoT is so ubiquitous today that most smart city dwellers may encounter, at the very least, three to four smart, connected devices or applications even before their day has begun in earnest. Smart speakers, smart health wearables, smartwatches, smart thermometers, smartphones, and computer vision-based CCTV cameras are a part of almost everybody's lives in smart cities today. Also, the utility of IoT-based devices is not limited to just smart cities. IoT networks are designed to endlessly collect data for detailed analysis, forecasts, and decision-making. Therefore, the need for this data to be accurate, consistent, constantly updated, and complete is critical for the massive global population that uses IoT-based devices in one way or another [13].
Here are some of the ways with which the data integrity in IoT networks can be consistently maintained.

BY USING EDGE DATA ANALYTICS FOR IOT NETWORKS

Even though data capturing sensors, applications and devices are scattered everywhere, transferring large amounts of data through a widespread IoT network can still be a cumbersome affair. Transferring a terabyte of data through a 10 MBPS broadband network can take about nine days. Additionally, there are always risks of data manipulation, distortion, loss, or breach during transmission via a large IoT network spread over vast distances.
To overcome this problem, businesses or smart city public agencies can implement edge AI, IoT, and computing tools for more bringing analytics closer to the data collection sources. Edge IoT analytics necessitate the use of lightweight software to enable the low-powered IoT nodes and gateways to capture data and perform query processing with precision. Additionally, the use of edge AI will facilitate faster analysis of data.
Most importantly, the use of edge IoT analytics safeguards the collected data from manipulation, loss, and breaches [14].

BY UPDATING IOT DEVICES AND NETWORKS REGULARLY

Regular usage can take its toll on heavily-used IoT devices over a period. Therefore, such devices must be regularly updated and patched to keep their performance and reliability consistently high. Regular updates enable businesses and smart city public agencies to maintain the scalability and data security of sensitive IoT networks. From a cybersecurity point of view, regular patching keeps IoT devices and data protected against new cyber threats[15].
Data consistency, coherence, and security are among the primary reasons for implementing IoT. By employing the measures listed above, the data integrity in IoT networks can be maintained seamlessly.

VII. PROBLEMS & RISKS WITH GOING GREEN

We're overwhelmed: The problems we face are so big, ocean acidification, massive extinctions, climate change, fresh water shortages that it already seems too little too late for a lot of these things. We have no idea where to start.

We're brainwashed: Most of us were brought up as consumers who spent a lot of time and energy thinking about buying things even as kids.

We don't think our actions will make any difference: Our thoughts changing a light bulb will not save the planet. Using a cloth bag will not save the plant etc. Our individual ability to improve a huge, widespread, complex problem is limited.

We're Too Busy: It takes a certain amount of emotional space and head space to care about something as abstract as the environment. Our lives are hectic as it is with other concerns to have any room left to care about something that seems far away and only tangentially connected to our daily life.

A risk is a vulnerability that could allow loss of confidentiality, integrity, or availability of computer services and where there is a possibility of the vulnerability being exploited. There are many things that are considered to be computer security risks. The foremost risk would probably come from malicious code like Viruses, Spyware, and Trojan horses. These can be infected on a system or number of systems through exploits in operating system software or web browsing software. Also, a common trend is a technique known as "phishing" where a spammer will send an email that looks like it's from someone else and by clicking on a link/opening an attachment you may be downloading malware. Some forms of malware can "phone home" back to the attacker which is how bot-nets are created which can be used to take down entire websites or be used as a launch pad to send lots of spam. The biggest computer security risk is actually the user behind the computer in most cases. That is why it is important to practice safe internet habits and keep virus protection up to date [16].

VIII. CONCLUSION

Serverless green cloud computing is a new paradigm in cloud computing, where the cloud service provider manages the resource allocation and pricing is based on actual usage. serverless computing started moving into the focus of the industry as the concept is promising and major public cloud service providers have been pushing their runtime models to the market. Serverless green cloud computing is seen as a chance for substantial cost reduction of cloud applications. Although the cost model is more complex, besides low usage applications, especially bursty and compute-intensive application benefit from the serverless computing.

REFERENCES

[1] Liu, P. (2020). Public-Key Encryption Secure Against Related Randomness Attacks for Improved End-to-End Security of Cloud/Edge Computing. IEEE Access, 8, 16750-16759.

[2] Li, J., Wang, S., Li, Y., Wang, H., Wang, H., Wang, H., ...& You, Z. (2019). An efficient attribute-based encryption scheme with policy update and file update in cloud computing. IEEE Transactions on Industrial Informatics, 15(12), 6500-6509.

[3] Fischlin, M., & Günther, F. (2020, February). Modeling memory faults in signature and authenticated encryption schemes. In Cryptographers' Track at the RSA Conference (pp. 56-84). Springer, Cham.

[4] Zhou, Y., Li, Z., Hu, F., & Li, F. (2019). Identity-based combined public key schemes for signature, encryption, and signcryption. In Information Technology and Applied Mathematics (pp. 3-22). Springer, Singapore.

[5] Prasad, A., & Kaushik, K. (2019). Digital Signatures. Emerging Security Algorithms and Techniques, 249.

[6] Prasetyadi, G., Hantoro, U. T., Mutiara, A. B., Muslim, A., & Refianti, R. (2019, October). Heresy: A Serverless Web Application to Store Compressed and Encrypted Document in the Form of URL. In 2019 Fourth International Conference on Informatics and Computing (ICIC) (pp. 1-5). IEEE.

[7] Li, Y., Yu, H., Song, B., & Chen, J. (2019). Image encryption based on a single-round dictionary and chaotic sequences in cloud computing. Concurrency and Computation: Practice and Experience, e5182.

[8] Shobana, R, Shalini, KS, Leelavathy, S and Sridevi, V 2016, "De duplication of data in cloud", International Journal of Chemical Sciences, vol. 14, no. 4, pp. 2933-2938, ISSN: 2523-6075.

[9] Stojmenovic, I and Wen, S 2014, "The fog computing paradigm: Scenarios and security issues", in Federated Conference on Computer Science and Information Systems (FedCSIS), pp. 1-8.

[10] Tharunn, G, Kommineni, G, Varma, SS and Verma, AS 2015, "Data deduplication in cloud storage", International Journal of Advanced Engineering and Global Technology, vol. 3, no. 8, pp. 1062-1065, ISSN: 2309-4893.

[11] Wang, H., Qin, Y., Huang, Y., Wang, Z., & Zhang, Y. (2017). Multiple image encryption and authentication in interference-based scheme by aid of space multiplexing. Optics & Laser Technology, 95, 63-71.

[12] Zhou, Y., Li, Z., Hu, F., & Li, F. (2019). Identity-based combined public key schemes for signature, encryption, and signcryption. In Information Technology and Applied Mathematics (pp. 3-22). Springer, Singapore.

[13] Aishwarya Shekhar, A Very Robust Dedicated and Verified Technique by Applying the Hybridity of Cloud for Deduplication of Data: IJTRE,2016.

[14] Aishwarya Shekhar, Analysis on improving energy efficiency in green cloud computing for IoT devices: IJTRE,2023.

[15] Aishwarya Shekhar,Analysis on Trust management serverless techniques for green cloud computing and internet of things: IJEAM,2023.

[16] A.Arulprakash, Dr.K.SampathKumar, "Improved Data Integrity in Cloud Serverless Environment Using Filter Based Approach" in Solid State Technology, Volume 64, No. 2 (2021) (Scopus) .

