International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Fog Computing Mitigate Limitations of Cloud Computing

Madhulika Bhatia, Shubham Sharma, Surbhi Bhatia, Mohammed Ali Alojail

Abstract: ***In today's world, cloud computing is the most exciting and advanced technology. It came into existence with lots of advantages, but cloud-only computing has some disadvantages also like latency in real-time data processing, network congestion, less bandwidth utilization, fault tolerance, and security issues in public cloud. To address the issue of real-time data-processing and security in public cloud new computing model are used which is known as Fog Computing. It is nearer to the client or edge so that it can reduce the latency in real time data-processing and security in public cloud using techniques like user profiling and decoying technique. Fog Computing help us to overcome the latency and security issues of cloud computing. It reduces cloud latency in real time data-processing because fog computing model is nearer to the edge devices. It also improves cloud security in the public cloud.***

Keywords : Cloud Computing, Fog Computing, Cloud Security

I. INTRODUCTION

Cloud Computing is an advanced computational model and it is defined as a ubiquitous, on-call network entry to a share collection of organizing computing resources which can be delivered to its end user with minimal management effort. It comes into the market with lots of advantages and changes the way of accessing computers, but it has some disadvantages also like slow response time, fault tolerance, less bandwidth utilization and security in the public cloud. To reduce the disadvantages of cloud-only computing a new computational model is suggested as fog computing[1].

Fog computing bring capabilities of cloud-like cloud intelligence down from the cloud close to the end user. Cellular base stations, Network routers, Wi-fi Gateways will be capable of running applications. End devices, like sensors, can perform basic data processing. Processing close to devices lowers the response time, enabling real-time application[2].

Manuscript published on January 30, 2020.
* Correspondence Author
Dr.Madhulika Bhatia*,Amity School of Engineering and Technlogy, Computer Science & Ebgineering, Amity University,Noida,India..Email: madhulikabhatia@gmail.com
Shubham Sharma, MRIIRS, Faridabad, Haryana, Email: xyz2@blueeyesintlligence.org
Dr. Surbhi Bhatia, CCSIT Department, King Faisal University, Saudi Arabia, sbhatia@kfu.edu.sa
Dr. Mohammad Alojail, CCSIT Department, King Faisal University, Saudi Arabia, malojail@kfu.edu.sa

Fog computing validates some of the agreement of data as well as resources at the network edge of the cloud, rather than building channels for cloud storage and application. Fog computing reduces the need for bandwidth by not passing every bit of information over the cloud, and instead of collecting it at certain access points. This kind of distributed strategy may help in lowering cost, reducing latencies and improve efficiencies.

A. Current System

The current cloud system gives only single user authentication which is not much secure. The attacker easily gets into the cloud and access files from the cloud may be those files contains confidential data. The current system doesn't check whether the user is authorized or not. The current system provides encryption technology for data security, but it is failing to secure the cloud as shown in Fig 1.

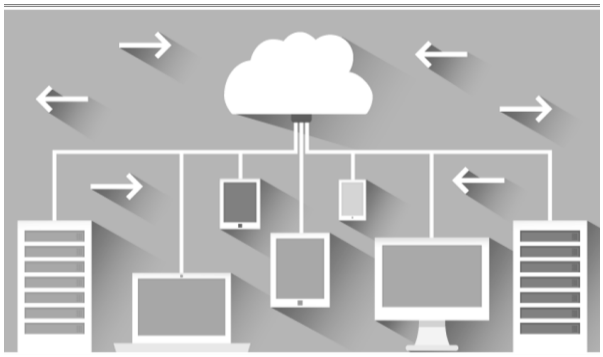

Fig.1. Existing computational model for cloud[4]

B. Security issues of Cloud Computing Current System in Public Cloud

- Security in public cloud is the main concern because the cloud follows the multi- tenant model.
- Public cloud is cheap, but security always restricts its adaptation from end-user point of view.
- Real-time Data processing is not possible in a current cloud model.
- Cloud model has high latency; therefore, it doesn't suit for real-time IOT devices.

II. RELATED WORK

Fog Computing is a computing model that enhances cloud-only computing services to the edge of the network. Recent Developments of Fog Computing are:

A. Smart Cities

There are many challenges in big cities that have various challenges like traffic congestion, safety issues of public, energy usage, issues related to sanitation and in providing simple municipal services. All these issues and challenges are pursued and taken care and solved within a single IoT network by installing a network of fog nodes.

A lack of network connectivity and low bandwidth utilization is a major issue in building smart cities.
Deploying a fog computing architecture allows for fog nodes to provide local processing and storage. This optimizes network usage.
Smart cities also face problems related to real time decision making which is quite impractical with cloud-only computing because it is not possible to send every bit of data over the cloud for making the decision, therefore, we need some fog nodes where we process the data and give response in minimum time[3].

B. Smart Buildings

Smart Buildings mean when the building can talk to a human and remind them to take a decision and sometimes it takes the decision of its own without human intervention. Today we can use lots of sensors in buildings for a different purpose, for example, we can use the ultrasonic sensor on the tank which can sense tank is fill complete and off the motor. Smoke sensors can also use in Smart Buildings. But if we have a building of 24 floors having 30 rooms on every floor then sensing data and sending every bit of it on cloud is quite impractical and it will take a lot of time in response.
To reduce the response time, we can use fog with cloud computing, and we can distribute our work in different fog node so that it can reduce the latency[4].

C. Visual Security

Visual Security is dominating today, everywhere we are surrounded by cameras whether in parking, metros, lifts, corridors, malls, outside our homes or even on roads there is a camera which is observing each action. We are collecting a large amount of data from these cameras but if we are not applying analytics on it then it is waste for us, therefore, we need to apply some type of analytics in these videos to extract information from them. Since videos require more bandwidth and it is quite impossible to transfer all data(videos) to the cloud for real-time intuition.
Here we need to detect and response which is very slow with cloud-only computing, therefore, we distribute the work among different fog nodes since they process data at network edge, therefore, it can give a response in less time [5].

III. FOG COMPUTATIONAL MODEL

There is an approach to secure cloud computing model using fog computing. Fog Computing is not a substitution for cloud computing. Fog or edge devices are there to help the cloud data center to better response time for real-time applications. Handshaking among Fog and Cloud computing is needed as shown in Fig 2. Fog Computing is just another layer between cloud and clients which bring capabilities of cloud nearer to the edge devices.

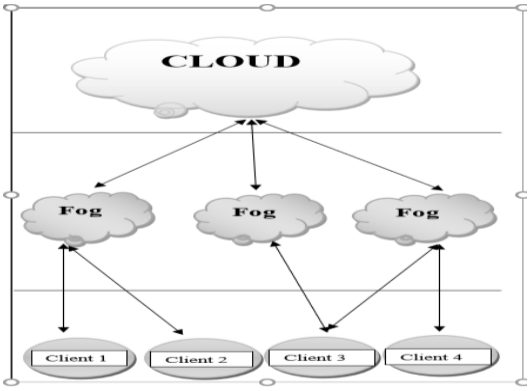

Fig 2. Fog Computing Model

A. Fog Computing Enablers

- **Virtualization**: Virtual machines can be used in edge devices[6].
- **Containers**: Reduces the overhead of resource management by using light-weight virtualizations. Example: Docker containers [7].
- **Service Oriented Architecture (SOA):** There is a protocol which helps in communication on network. With the help of this and Service-oriented Architecture which is a model of designing software where services are provided to the other components by application components[8].
- **Software Defined Networking:** Software-defined networking (SDN) is a way to using open protocols, such as OpenFlow, to implement globally available software control at the edges of the network to access network switches and routers that typically would use closed and proprietary firmware[9]

IV. TECHNIQUES USED TO SECURE CLOUD WITH FOG

It is a way of behavior-based security is commonly used in fraud detection application. In User profiling based on user behavior his action is predictable and if there is any deviation in his action it means it's an unauthorized user.
This technique basically observes the users search behavior's it can easily differentiate between normal user and unauthorized user as shown in Fig 3 [10].

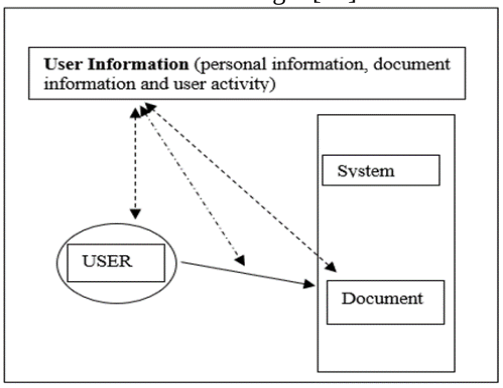

Fig 3: User Profiling

User activity is continuously track and match with user's previous information and if there is any suspicious event occur system generate alert.

A. Decoy Technique

It serves two purposes
1. Validating whether the data is authorized
2. Misleading the user with false or bogus information
In this technique if attacker who has bad intent may click on the bogus information and he believed that he gets important information and when the decoy document is downloaded an alert is generated and this notify the system with illegal activity as shown in Fig 4 [10].

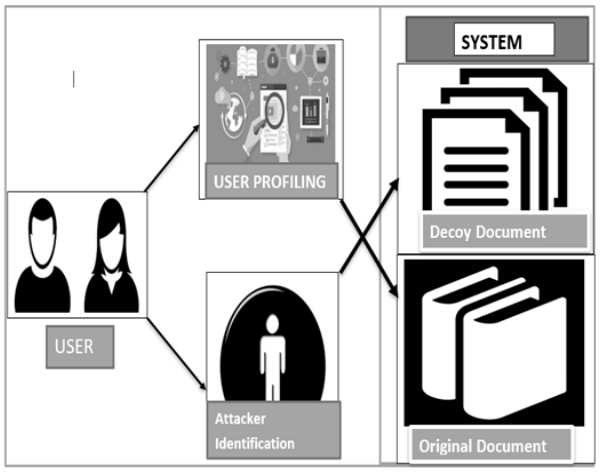

Fig 4: Decoy Technique

V. ALGORITHM

Algorithm for User Behavior Profiling
1. Identify which operation is executed
2. Track user profile consisting of the following parameters: username, password, user key specified during document access, type of document selected original or decoy.
3. At the time of login, password specified is tracked.
4. When the document is accessed by user key and it is tracked along with operation (legal or illegal).
5. Classify profile as legal user and illegal user using mathematical operation:
M(IV)=count (illegal operations of each type)/count (operations of each type). If the value of M(IV) is above threshold parameter, then the profile is categorized as invalid and the user is redirected to the decoy file [2]. Detailed methodology is shown Fig 5.

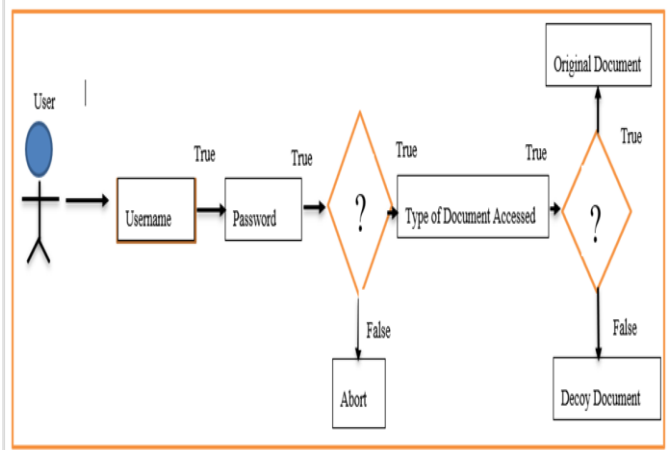

Fig 5: Algorithm

VI. RESULTS AND DISCUSSIONS

We have used FogSim open source tool to perform modeling and simulation of fog computing environment to obtain and evaluating management of resources as well implementing low-level scheduler as well upper scheduler in topology. We have taken basic scenario to implement topology with fog as well as low level scheduler and upper level scheduler.
Various devices in topology are connected to wireless link with data center connected to upper and low level scheduler then they all are connected to various gadgets like mobile phone, data sensors etc. Simulation Topology has been shown in Fig 6.

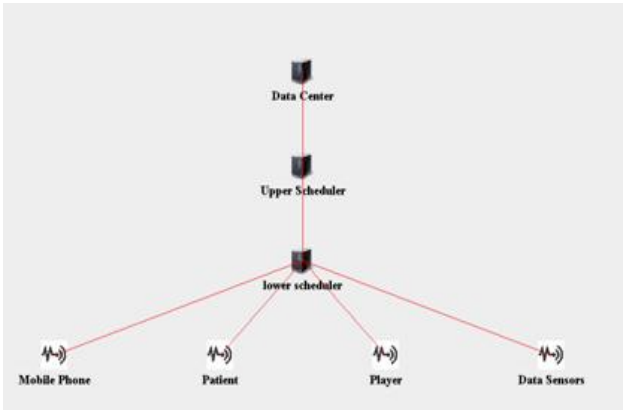

Fig 6: Simulation

Fog devices has been added as Data center, Upper scheduler and Data sensors as shown in Fig 7a) , 7b) and 7c).

Fig 7a) Data center

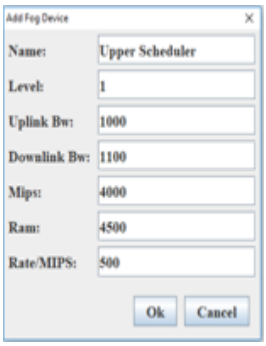

Fig 7b) Upper Scheduler

Fig 9a) Topology Phase 1

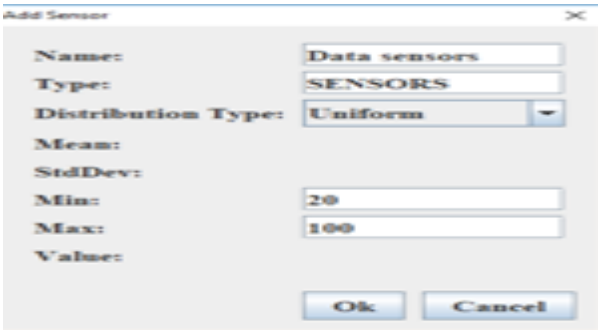

Fig 7c) Data sensors

Then Latency has been added as 50 clock period as shown in Fig 8.

Fig 8 Latency as 50 clock period

The topology is executed in FogSim and extracted in Eclipse IDE as shown in Fig 9 a)Phase 1, b)Phase 2 and c) Phase 3

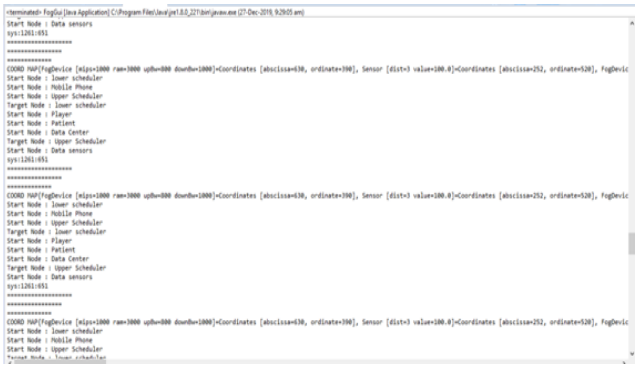

Fig 9b) Topology Phase 1

Fig 9c) Topology Phase 1

VII. FUTURE SCOPE

We can apply user behavior profiling and decoy technique for fog computing to protect a different type of data like images, multimedia files,.txt files, .docs files, etc. Data can be divided and stored in a different cloud to provide additional security. These two-technology user behavior profiling and decoy technique provide security to the cloud. In future fog computing model best suit for real-time systems like IOT devices and embedded systems. If the attack occurs, then the attacker must satisfy with decoy information and original information is remain protected in the cloud with the help of fog Computing model.

IX. CONCLUSION

In this paper, we propose how we can mitigate the limitations of the cloud using fog. Fog Computing reduces cloud latency because now most of the data processing is done on the network edge because of which it suits best for real-time applications as well. Fog computing helps to increase cloud security using user behavior profiling and decoy technique. If unauthorized access is recognized, then we duplicate the data and store it on the cloud which provides an additional layer of security.

REFERENCES

1. De Donno, M., Tange, K., & Dragoni, N. (2019). Foundations and Evolution of Modern Computing Paradigms: Cloud, IoT, Edge, and Fog. Ieee Access, 7, 150936-150948.
2. Chen, Z., Dong, W., Li, H., Zhang, P., Chen, X., & Cao, J. (2014). Collaborative network security in multi-tenant data center for cloud computing. Tsinghua Science and Technology, 19(1), 82-9.
3. Cheng, B., Solmaz, G., Cirillo, F., Kovacs, E., Terasawa, K., & Kitazawa, A. (2017). FogFlow: Easy programming of IoT services over cloud and edges for smart cities. IEEE Internet of Things Journal, 5(2), 696-707.
4. Cheng, B., Solmaz, G., Cirillo, F., Kovacs, E., Terasawa, K., & Kitazawa, A. (2017). FogFlow: Easy programming of IoT services over cloud and edges for smart cities. IEEE Internet of Things Journal, 5(2), 696-707.
5. Sultana, T., & Wahid, K. A. (2019). Choice of Application Layer Protocols for Next Generation Video Surveillance Using Internet of Video Things. IEEE Access, 7, 41607-41624.
6. Varghese, B., Reaño, C., & Silla, F. (2018). Accelerator Virtualization in Fog Computing: Moving from the Cloud to the Edge. IEEE Cloud Computing, 5(6), 28-37.
7. Xavier, M. G., Neves, M. V., Rossi, F. D., Ferreto, T. C., Lange, T., & De Rose, C. A. (2013, February). Performance evaluation of container-based virtualization for high performance computing environments. In 2013 21st Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (pp. 233-240). IEEE.
8. Ouda, A. H., Allison, D. S., & Capretz, M. A. (2010, July). Security protocols in service-oriented architecture. In 2010 6th World Congress on Services (pp. 185-186). IEEE.
9. Huang, L., Li, G., Wu, J., Li, L., Li, J., & Morello, R. (2016, October). Software-defined QoS provisioning for fog computing advanced wireless sensor networks. In 2016 IEEE SENSORS (pp. 1-3). IEEE.
10. Stolfo, S. J., Salem, M. B., & Keromytis, A. D. (2012, May). Fog computing: Mitigating insider data theft attacks in the cloud. In 2012 IEEE symposium on security and privacy workshops (pp. 125-128). IEEE.
11. Reena, K. M., Yadav, S. K., Bajaj, N. K., & Singh, V. (2017, March). Security implementation in cloud computing using user behaviour profiling and decoy technology. In 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT) (pp. 471-474). IEEE.

12. Kaur, R., & Kaur, J. (2015, March). Cloud computing security issues and its solution: A review. In 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 1198-1200). IEEE..

AUTHORS PROFILE

Dr. Madhulika Bhatia is working as a Associate Professor in Department of Computer Science and Engineering at Amity School of Engineering and Technology, Amity University, Noida. She holds Diploma in Computer Science & Engineering, B.E in Computer Science & Engineering ,MBA in Information Technology, M.Tech in Computer Science & Ph.D from Amity University, Noida. She has total 14 years of Teaching experience. She published almost 32 Research Papers in National, International conferences and Journals. She is also Author of two Books. She Filed three Provisional Patent. She attended and organized many workshops, Guest Lectures, seminars. She is also member of many Technical societies like IET,ACM , UACEE. She reviewed for Elsevier-Heliyon, IGI, Indian Journal of Science and Technology, Wiley and completed editorial for Springer Nature, Switzerland Title" Data Visualization and Knowledge Engineering". She is Recently nominated as Brand ambassador representing India for Bentham Science publishers. Her Innovative Project startup Idea "Abodsy private limited" get Selected at Startup Event Connecting East & West | Startup Istanbul 2019 among 155.279 startup applications and is selected among Top 100 Demo Day at Istanbul in october,2019.

Shubham Sharma, is pursuing B.Tech in Computer Science & Engineering with specialization in Cloud Computing with IBM at Manav Rachna International Institute of Research & Studies, Faridabad. He has participated in many conferences & workshops and published research papers in International Conferences. He is placed with TCS, India.

Dr. Surbhi Bhatia, is an Assistant Professor in Department of Information Systems, College of Computer Sciences and Information Technology, King Faisal univesity, Saudi Arabia. She has rich 8 years of teching and academic experience. She recieved her Ph.D. from Banasthali vidyapith, Rajasthan in 20018. She is in the Editorial board member with Inderscience Publishers in the International Journal of Hybrid Intelligence. She has published two patents with Government of india. She has published 20 papers in reputed journals and conferences in high indexing databases. She has successfully published many book chapters indexed in major indexing databases. She has developed "Information Retrieval System using Opinion Mining" during 2014-2018. She has supervised research projects at UG and PG level. Her research areas include, Databases, Data mining and Machine Learning

Dr. Mohammad Alojail, is Doctorate in Information systems from RMIT University, Australia. He is presently the Chairman of Information System Department, College of Computer Sciences and Information Technology, King Faisal University, Saudi Arabia. He is the Chairman and member of various committees. He is also the reviewer of International Journals and Conferences. Dr. Mohammad has published papers in high indexing .Databases. He has been an active member int he Accreditation team. He has considerable Experience in the field of Information systems. He has delivered number of talks on leadership and management and successfully led and mange teams to deliver large-scale industrial projects. Dr. Alojail has written many scholarly papers in the field of IS and IT outsourcing.

.