International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Working of Fog Computing & It's Principles

[1]R.J. Malleswari Devi, [2]D. Maneesha, [3]B. Sai Sahithi, [4]K. Kalyani, [5]V. Lakshmi Vasavi

[1,2,3,4,5] Santhiram Engineering College

ABSTRACT

Nowadays huge amount of data is stored on cloud. Cloud computing promises to significantly change the way we use computers and access and store our personal and business information. Because of these new computing and communication paradigm there arise data security challenges. In this paper, we proposed a system for securing data stored in the cloud using decoy technology. In this we monitor data access in the cloud and detect abnormal data access. When unauthorized access is detected that users activity will be tracked in log details table. Based on the activities performed by unauthorized user admin can blocked or delete that user.

When a new user enters into this System, he have to register first. After successfully registered, that user will get a key through mail. And during login, if the user enter wrong password continuously more than three times, he will get access and his activity will be tracked on log details table in the database. (that is in the action column trialpwd will be entered).And after this , whatever activities he is doing that also will be tracked in the log table .If he downloads any file, he won't get original file. Instead of that he will get decoy file. If a user entered correct password and he will get access .If that user wants to download any file, and he entered wrong key more than three times, in first three cases in the action column invalid will be entered and in the fourth case wrong key and that user will get decoy file .In every case it Now will execute user behaviour algorithm. When a user edit password he enters wrong key more than three times , then edit pwd wrong key will be entered. And user will get message that password updated successfully. But in actual case it is not updating.

1. INTRODUCTION

Cloud computing is achieving popularity and gaining attention in business organizations. It offers a variety of services to the users. It is an ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources . Due this ease, software companies and other agencies are shifting more towards cloud computing environment.

To achieve better operational efficiency in many organizations and small or medium agencies is using Cloud environment for managing their data. Cloud Computing is a combination of a number of computing strategies and concepts such as Service Oriented Architecture (SOA), virtualization and other which rely on the Internet.

It is considered as a delivery platform in which resources are provided as a service to the client through the Internet. Although, Cloud Computing provides an easy way for accessing, managing and computation of user data, but it also has some severe security risks. There are some traditional security mechanism such as identity, authorization and authentication, but now these are not sufficient .

Fog computing, also known as fogging, is a model in which data, processing and applications are concentrated in devices at the network edge rather than existing almost entirely in the cloud. Cloud computing promises to significantly change the way we use computers and access and store our personal and business information. Because of these new computing and communication paradigm there arise data security challenges. Even though existing techniques use security mechanisms, data theft attacks prevention fails. To overcome this we can use decoy technology to secure data stored in cloud.

2. FOG COMPUTING

Fog computing is a paradigm which extends cloud computing paradigm to the edge of the network. Terms Edge Computing and Fog Computing are often used interchangeably. Fog provides data, compute, storage, and application services to end-users Enables new breed of applications and services.

Fog computing is a distributed paradigm that provides cloud-like services to the network edge. It leverages cloud and edge resources along with its own infrastructure, as Figure 1 shows. In essence, the technology deals with IoT data locally by utilizing clients or edge devices near users to carry out a substantial amount of storage, communication, control, configuration, and management. The approach benefits from edge devices' close proximity to sensors, while leveraging the on demand scalability of cloud resources.

Fog computing—which seamlessly integrates edge devices and cloud resources—helps overcome these limitations. It avoids resource contention at the edge by leveraging cloud resources and coordinating the use of geographically distributed edge devices.

2.1. Working:

- We monitor data access in the cloud and detect abnormal data access patterns. When unauthorized access is suspected and then verified using challenge questions.

- We launch a disinformation attack by returning large amount of decoy information to the attacker. This protects against the misuse of the user's real data.

3. ARCHITECTURE OF FOG COMPUTING

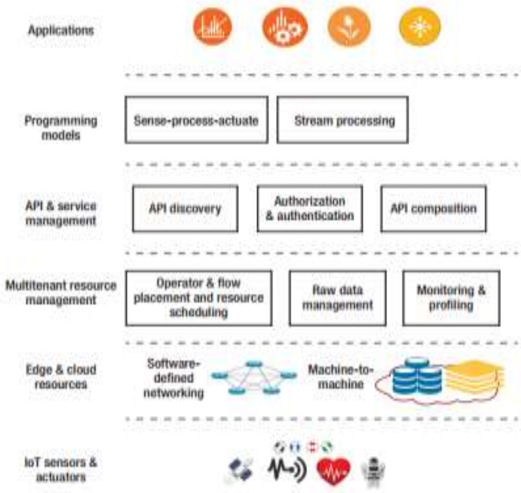

Figure1: - Architecture of fog computing

- ➢ In the bottom layer are end devices—including sensors and actuators—along with applications that enhance their functionality.
- ➢ These elements use the next layer, the network, for communicating with edge devices, such as gateways, and then with cloud services.
- ➢ The resource-management layer runs the entire infrastructure and enables quality-of-service enforcement. Finally, applications leverage fog-computing programming models to deliver intelligent services to users.

4. FOG COMPUTING COMPONENTS

Figure 1 presents a fog-computing reference architecture. Fog systems generally use the sense-process-actuate and stream-processing programming models. Sensors stream data to IoT networks, applications running on fog devices subscribe to and process the information, and the obtained insights are translated into actions sent to actuators.

Fog systems dynamically discover and use APIs to build complex functionalities. Components at the resource-management layer use information from the resource monitoring service to track the state of available cloud, fog, and network resources and identify the best candidates to process incoming tasks. With multitenant applications, the resource-management components prioritize the tasks of the various participating users or programs.

Edge and cloud resources communicate using machine-to-machine (M2M) standards such as MQTT (formerly MQ Telemetry Transport) and the Constrained Application Protocol (CoAP). Software-defined networking (SDN) helps with the efficient management of heterogeneous fog networks.

The following are the components of fog computing.

- IoT sensors & actuators
- Edge & cloud resources
- Multitenant resource management
- API & service management
- Programming models
- Applications.

5. FOG COMPUTING SOFTWARE SYSTEMS

There are four prominent software systems for building fog computing environments and applications. Cisco IOx provides device management and enables M2M services in fog environments.5 Using device abstractions provided by Cisco IOx APIs, applications running on fog devices can communicate with other IoT devices via M2M protocols.

Cisco Data in Motion (DMo) enables data management and analysis at the network edge and is built into products that Cisco Systems and its partners provide. LocalGrid's fog-computing platform is software installed on network devices in smart grids. It provides reliable M2M communication between devices and data-processing services without going through the cloud. Cisco ParStream's fog-computing platform enables real-time IoT analytics.

5.1. MODELING AND SIMULATION:

To enable real-time analytics in fog computing, we must investigate various resource-management and scheduling techniques including the placement, migration, and consolidation of stream-processing operators, application modules, and tasks.

This significantly impacts processing latency and decision-making times. However, constructing a real IoT environment as a testbed for evaluating such techniques is costly and doesn't provide a controllable environment for conducting repeatable experiments.

To overcome this limitation, we developed an open source simulator called iFogSim.11 iFogSim enables the modeling and simulation of fog-computing environments for the evaluation of resource-management and scheduling policies across edge and cloud resources under multiple scenarios, based on their impact on latency, energy consumption, network congestion, and operational costs. It measures performance metrics and simulates edge devices, cloud datacenters, sensors, network links, data streams, and stream-processing applications.

6. CHALLENGES OF FOG COMPUTING

Realizing fog computing's full potential presents several challenges including balancing load distribution between edge and cloud resources, API and service management and sharing, and SDN communications. There are several other important examples.

Enabling real-time analytics:

In fog environments, resource management systems should be able to dynamically determine which analytics tasks are being pushed to which cloudor edge-based resource to minimize latency and maximize throughput. These systems also must consider other criteria such as various countries' data privacy laws involving, for example, medical and financial information.

Programming models and architectures:

Most stream- and data-processing frameworks, including Apache Storm and S4, don't provide enough scalability and flexibility for fog and IoT environments because their architecture is based on static configurations. Fog environments require the ability to add and remove resources dynamically because processing nodes are generally mobile devices that frequently join and leave networks.

Security, reliability, and fault tolerance:

Enforcing security in fog environments—which have multiple service providers and users, as well as distributed resources—is a key challenge. Designing and implementing authentication and authorization techniques that can work with multiple fog nodes that have different computing capacities is difficult. Public-key infrastructures and trusted execution environments are potential solutions.12 Users of fog deployments also must plan for the failure of individual sensors, networks, service platforms, and applications. To help with this, they could apply standards, such as the Stream Control Transmission Protocol, that deal with packet and event reliability in wireless sensor networks.

Power consumption:

Fog environments consist of many nodes. Thus, the computation is distributed and can be less energy efficient than in centralized cloud systems. Using efficient communications protocols such as CoAP, effective filtering and sampling techniques, and joint computing and network resource optimization can minimize energy consumption in fog environments.

Fog computing enables the seamless integration of edge and cloud resources. It supports the decentralized and intelligent processing of unprecedented data volumes generated by IoT sensors deployed for smooth integration of physical and cyber environments. This could generate many benefits to society by, for example, enabling smart healthcare applications. The further development of fog computing could thus help the IoT reach its vast potential.

7. FOG COMPUTING APPLICATIONS

Various applications could benefit from fog computing.

7.1. Healthcare and activity tracking:

Fog computing could be useful in healthcare, in which real-time processing and event response are critical. One proposed system utilizes fog computing to detect, predict, and prevent falls by stroke patients. The fall-detection learning algorithms are dynamically deployed across edge devices and cloud resources. Experiments concluded that this system had a lower response time and consumed less energy than cloud only approaches. A proposed fog computing–based smart-healthcare system enables low latency, mobility support, and location and privacy awareness.

7.2. Smart utility services:

Fog computing can be used with smart utility services,8 whose focus is improving energy generation, delivery, and billing. In such environments, edge devices can report more finegrained energy-consumption details (for example, hourly and daily, rather than monthly, readings) to users' mobile devices than traditional smart utility services.These edge devices can also calculate the cost of power consumption throughout the day and suggest which energy source is most economical at any given time or when home appliances should be turned on to minimize utility use.

7.3. Augmented reality, cognitive systems, and gaming:

Fog computing plays a major role in augmented-reality applications, which are latency sensitive. For example, the EEG Tractor Beam augmented multiplayer, online brain–computerinteraction game performs continuous real-time brain-state classification on fog devices and then tunes classification models on cloud servers, based on electroencephalogram readings that sensors collect.9 A wearable cognitive-assistance system that uses Google Glass devices helps people with reduced mental acuity perform various tasks, including telling them the names of people they meet but don't remember.10 In this application, devices communicate with the cloud for delay-tolerant jobs such as error reporting and logging.

8. MODULES OF FOG COMPUTING

1. User Authentication:

The user is facilitated here to authenticate and thus, ensure that only valid users can access the application. But, it also tracks the user login operation and accordingly redirects the user to the decoy application.

2. Admin Module:

This module facilitates the admin to manage users, the data stored and the invalid activities occurring within the application. Thus, this user will be responsible for tracking the application functionalities. A set of valid access rules will also be defined by the admin for identification of invalid users.

3. File Access Module:

This module will enable to track whether the search operations executed by the user follow a valid set of operations or not. Accordingly, the system will decide whether the user should be redirected to the decoy environment.

4. Data Access Module:

The data available for user access will be authenticated using a separate user key specified by the application to the user during registration. Based on the validity of this user key the system will redirect the user to the Decoy Module for tracking and prevent invalid distribution of data.

5. Decoy Module:

This module will facilitate the system to redirect invalid users to a dummy set of modules wherein invalid data will be distributed to the invalid user and the user activities will be notified to the admin. Thus, the system will not notify the invalid user about the detection of invalid activity and prevent.

9. INTERNET OF THINGS

The Internet of Things (IoT) represents a new world of information and communication technologies (ICTs) from anytime, anyplace connectivity for anyone. All Things in Internet of things or IoT are uniquely addressable and are connected using standard communication protocols. It will consist of connections that will multiply and create entirely new dynamic network of networks.

The Internet of things (IoT) is the inter-networking of physical devices, vehicles buildings,andotheritems embedded with electronics, software, sensors, actuators, networkconnectivity which enable these objects to collect and exchange data. The IoT allows objects to be sensed or controlled remotely across existing network infrastructure,[4] creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention.

When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, virtual power plants, smart homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of about 30 billion objects by 2020.

"Things", in the IoT sense, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, DNA analysis devices for environmental/food/pathogen monitoring, or field operation devices that assist firefighters in search and rescueoperations. Legal scholars suggest regarding "Things" as an "inextricable mixture of hardware, software, data and service".

9.1 TECHNOLOGY ROADMAP OF INTERNET OF THINGS :

In the future the Internet of things may be a non-deterministic and open network in which auto-organized or intelligent entities (Web services, SOA components), virtual objects (avatars) will be interoperable and able to act independently (pursuing their own objectives or shared ones) depending on the context, circumstances or environments. Autonomous behavior through the collection and reasoning of context information as well as the objects ability to detect changes in the environment, faults affecting sensors and introduce suitable mitigation measures constitute a major research trend,[103] clearly needed to provide credibility to the IoT technology.

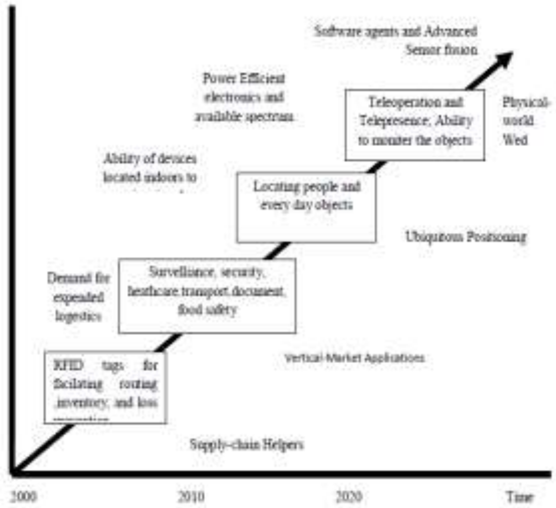

Figure2: Technology roadmap of Internet of Things

- No of end devices that are connected to internet are expected to rise above 50+ billion by 2020.
- cloud computing architectures won't be able to handle the demand of the Internet of things
- So only cloud is not the optimal solution to handle this massive explosion.
- Fog is needed in between to optimize – need for an interplay of cloud and fog.

10. INTERNET OF THINGS DEVICES APPLICATIONS AND EXAMPLES

You've likely heard the term "Internet of Things" at some point from a colleague, an article, or an advertisement. But the term is broad and can cover an overwhelming amount of information.

In short, the Internet of Things refers to the rapidly growing network of connected objects that are able to collect and exchange data using embedded sensors. Thermostats, cars, lights, refrigerators, and more appliances can all be connected to the IoT.

To help clarify how the Internet of Things works, we've laid out some applications for the IoT, along with some specific devices and examples.

10.1. Applications of the Internet of Things:

Smart Home:

The smart home is likely the most popular IoT application at the moment because it is the one that is most affordable and readily available to consumers. From the Amazon Echo to the Nest Thermostat, there are hundreds of products on the market that users can control with their voices to make their lives more connected than ever.

Wearable's:

Watches are no longer just for telling time. The Apple Watch and other smartwatches on the market have turned our wrists into smartphone holsters by enabling text messaging, phone calls, and more. And devices such as Fitbit and Jawbone have helped revolutionize the fitness world by giving people more data about their workouts.

Smart Cities:

The IoT has the potential to transform entire cities by solving real problems citizens face each day. With the proper connections and data, the Internet of Things can solve traffic congestion issues and reduce noise, crime, and pollution.

Connected Car:

These vehicles are equipped with Internet access and can share that access with others, just like connecting to a wireless network in a home or office. More vehicles are starting to come equipped with this functionality, so prepare to see more apps included in future cars.

10.2. Internet of Things Devices & Examples:

Amazon Echo - Smart Home:

The Amazon Echo works through its voice assistant, Alexa, which users can talk to in order to perform a variety of functions. Users can tell Alexa to play music, provide a weather report, get sports scores, order an Uber, and more.

Fitbit One - Wearables:

The Fitbit One tracks your steps, floors climbed, calories burned, and sleep quality. The device also wirelessly syncs with computers and smartphones in order to transmit your fitness data in understandable charts to monitor your progress.

arcelona - Smart Cities:

The Spanish city is one of the foremost smart cities in the world after it implemented several IoT initiatives that have helped enhance smart parking and the environment.

AT&T - Connected Car:

AT&T added 1.3 million cars to its network in the second quarter of 2016, bringing the total number of cars it connects to 9.5 million. Drivers don't have to subscribe or pay a monthly fee for data in order for AT&T to count them as subscribers.

11. Use Case to Drive Fog computing

Use Case : A smart Traffic Light System (STLS)

To abstract the major requirements to propose an architecture that addresses a vast majority of the IoT requirements.

- STLS calls for deployment of a STL at each intersection.
- The STL is equipped with sensors that

1. Measure the distance and speed of approaching vehicles from every direction.

2. Detect presence of pedestrians/other vehicles crossing the street.

- Issues "Slow down" warnings to vehicles at risk to crossing in red and even modifies its own cycle to prevent collisions.
- STLS has 3 major goals:

1. Accidents prevention

2. Maintenance of steady flow of traffic(green waves along the main roads)

3. Collection of relevant data to evaluate and improve the system

Figure 3:- Smart Light Traffic System(STLS)

- Mobility, for instance, a critical attribute in Smart Connected Vehicle and Connected Rail, plays no role in STLS.
- Analyzing data close to the device that collected the data can make the difference between averting disaster and a cascading system failure.

12. CONCLUSION

We present an approach for securing business data in the cloud. Once unauthorized access or exposure is suspected, and later verified, with challenge questions for that instance, then we inundate the malicious insider with bogus information in order to dilute the user's real data. Fog computing enables the seamless integration of edge and cloud resources. It supports the decentralized and intelligent processing of unprecedented data volumes generated by IoT sensors deployed for smooth integration of physical and cyber environments. This could generate many benefits to society by, for example, enabling smart healthcare applications. The further development of fog computing could thus help the IoT reach its vast potential.

13. References

[1]. R. Buyya and A. Dastjerdi, Internet of Things: Principles and Paradigms, Morgan Kaufmann, 2016.

[2]. J. Manyika et al., Unlocking the Potential of the Internet of Things, McKinsey & Company, 2015.

[3]. R. Cortés et al., "Stream Processing of Healthcare Sensor Data: Studying User Traces to Identify Challenges from a Big Data Perspective," Procedia Computer Science, vol. 52, 2015, pp. 1004–1009.

[4]. W. Shi and S. Dustdar, "The Promise of Edge Computing," Computer, vol. 49, no. 5, 2016, pp. 78–81.

[5]. F. Bonomi et al., "Fog Computing: A Platform for Internet of Things and Analytics," Big Data and Internet of Things: A Roadmap for Smart Environments, N. Bessis and C. Dobre, eds., Springer, 2014, pp. 169–186.

[6]. Y. Cao et al., "FAST: A Fog Computing Assisted Distributed Analytics System to Monitor Fall for Stroke Mitigation," Proc. 10th IEEE Int'l Conf. Networking, Architecture and Storage (NAS 15), 2015, pp. 2–11.

[7]. V. Stantchev et al., "Smart Items, Fog and Cloud Computing as Enablers of Servitization in Healthcare," J. Sensors & Transducers, vol. 185, no. 2, 2015, pp. 121–128.

[8]. J. Li et al., "EHOPES: Data-Centered Fog Platform for Smart Living," Proc. 2015 Int'l Telecommunication Networks and Applications Conf. (ITNAC 15), 2015, pp. 308–313.

[9]. J. Zao et al., "Augmented Brain Computer Interaction Based on Fog Computing and Linked Data," Proc. 10th IEEE Int'l Conf. Intelligent Environments (IE 14), 2014, pp. 374–377.

[10]. K. Ha et al., "Towards Wearable Cognitive Assistance," Proc. 12th Int'l Conf. Mobile Systems, Applications, and Services (MobiSys 14), 2014, pp. 68–81.