An Opportunistic Resource Management Model to Overcome Resource-Constraint in the Internet of Things

Nader Sohrabi Safa[a], Carsten Maple[b], Mahboobeh Haghparast[c], *Tim Watson*[d], *Mehrdad Dianati*[e]
Cyber Security Centre, WMG, University of Warwick, Coventry, United Kingdom[a,b,d,e]
Department of Information Systems, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia[c]

Abstract

Experts believe that the Internet of Things (IoT) is a new revolution in technology and has brought many advantages for our society. However, there are serious challenges in terms of information security and privacy protection. Smart objects usually do not have malware detection due to resource limitations and their intrusion detection work on a particular network. Low computation power, low bandwidth, low battery, storage and memory contribute to a resource-constrained effect on information security and privacy protection in the domain of IoT. The capacity of fog and cloud computing such as efficient computing, data access, network and storage, supporting mobility, location awareness, heterogeneity, scalability and low latency in secure communication positively influence information security and privacy protection in IoT. This study illustrates the positive effect of fog and cloud computing on the security of IoT systems and presents a decision-making model based on the object's characteristics such as computational power, storage, memory, energy consumption, bandwidth, packet delivery, hop-count, etc. This helps an IoT system chooses the best nodes for creating the fog that we need in the IoT system. Our experiment shows that the proposed approach has less computational, communicational cost and more productivity in compare with the situation that we choose the smart objects randomly to create a fog.

Keywords: Fog, cloud, resource, information security, privacy, Internet of Things

Introduction

The Internet has provided a backbone for connecting different objects to each other and has changed human life significantly. The ubiquitous things is a new concept that has been created by the interconnection and intercommunication among smart objects [1]. We are faced with a huge volume of data in this environment. Network traffic, increasing demands of real time, latency-sensitive applications, resource-constraints (computational power, storage, memory, etc.) in actuators, mobility and geo-distribution of smart objects, and heterogeneity that are new challenges in the domain of IoT [2]. These weaknesses directly or indirectly influence information security and privacy violation in IoT systems [3].

Resource-constraint in actuators jeopardises secure communication between different smart objects [4]. Messages need to be sent encrypted; they will be decrypted for process in the target. The result of the process should be encrypted and send to the same object or other smart objects. We have latency; this delay not only creates risk for information security, it may also impact human safety in some applications of IoT, such as smart vehicles. Lightweight cryptography has been presented to overcome this challenge in vehicle-to-vehicle (V2V) communication, and in many other secure communications in IoT [5]. Smart objects usually do not have malware detection due to limitation in resources; their intrusion detection only can detect attacks in particular networks (not hybrid). These are examples of common problems in the IoT domain.

Cloud computing has been suggested to overcome these challenges due to its high computational power and its capacity in terms of resources [6]. Cloud computing is a centralised approach and productive in many cases such as smart grid, smart home and smart city and so forth; however, in many cases smart objects are mobile (smart vehicle, wearable devices, mobile etc.). The distance between objects and their movement besides network traffic encourages experts to find more effective solutions. Latency-sensitive applications have attracted the attention of experts in this domain [7]; many processes and data storage can be done at the local level to solve latency issues. A decision unit decides whether data should be sent to the cloud and saved for a longer time or kept at the local level (fog) to decrease latency in processes.

A cloudlet could be an initial solution to solve this problem, as it uses computational resources in the vicinity of users or smart devices in order to achieve local processes and overcome storage, network traffic and latency restrictions [8,9]. The optimal offloading algorithm helps cloudlets to achieve low cost in terms of computation and communication costs. However, as cloudlets use Wi-Fi for communication between smart devices this restricts its coverage area [10].

Fog computing is another effective and efficient approach that can address these limitations. Fog computing enables different heterogeneous devices at the edge of a network to connect to each other and collaborate in a geographical distributed system with optimal use of network, storage and other resources [11]. Fog computing extends cloud services to the edge of network; the local network edge devices provide data for Fog. This brings communication, computation, storage and control close to end-users and solves resource-constraint, network traffic issues and latency in IoT systems [12]. There are two views about fog and cloud computing in some applications of IoT in smart city or smart vehicle; in the traditional view, fog and cloud can be considered as an infrastructure that need we provide proper software and hardware and setup fog and cloud in smart city or in the roadsides. This process is time consuming and expensive. However, there is considerable resource available in edge devices that can be utilised to form an ad-hoc network to supplement to computation, memory, storage, bandwidth and so on in IoT applications [13]. In this research, we use the resources in the other smart objects that are in vicinity of the main actuator to overcome this challenge. Figure 1 shows the structure of fog and cloud computing in IoT in a concise form.

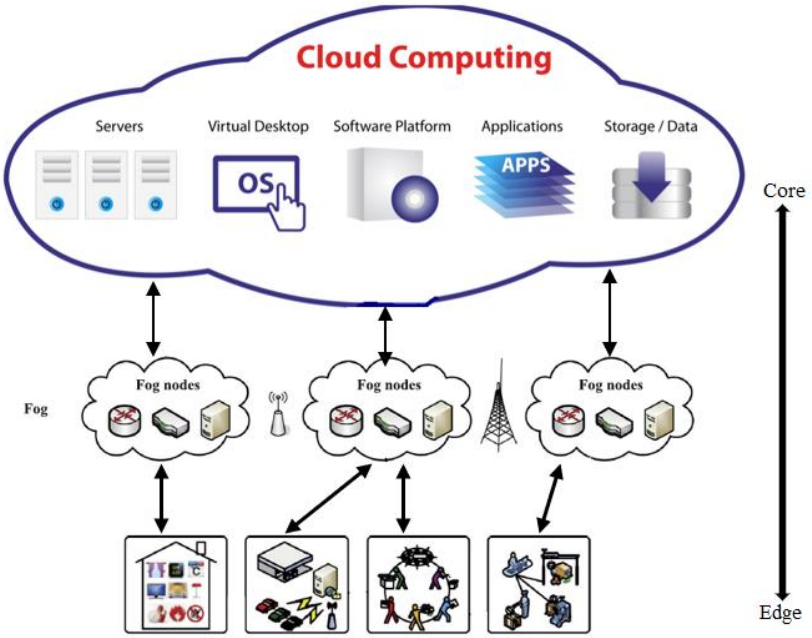

Figure 1: Fog and cloud Computing in IoT

Various devices can connect to the fog by different wireless connection such as Wi-Fi, Bluetooth and 4G to provide computation and storage if necessary. Fog nodes can connect to the cloud over the Internet when they need rich computing, storage or other resources. Fog computing approaches can deliver proper decision making and data analysis services with low latency [14].

Vulnerability in different layers of IoT

IoT systems usually collect and transfer data between different objects. Temperature, pressure, sound, vibration are examples of data that can be collected in a perception or physical layer. Different actuators connect to each other by network layer. The data can be transferred securely by the transport layer. Various applications in smart homes, smart cities, health, infrastructure and so on can provide useful services for users in the application layer. Table 1 shows different layers of an IoT system in a concise form.

Table 1

Information security and privacy protection can be compromised in different layers of IoT, from the perception layer to the network, transport and application layers. Andrea, Chrysostomou, Hadjichristofi [15] have presented a classification of attacks in IoT based on four layers of IoT - the perception or physical, network, software and encryption attacks. In this view IoT protocols play an important role in the encryption of data. Physical attacks usually occur when attackers are in the vicinity of IoT devices. The network attacks refer to the manipulation of IoT network systems that cause damage. Vulnerabilities in the design and implementation of IoT software can lead to successful software attacks. Encryption attacks relate to breaking the encryption system. These vulnerabilities originate from man-in-the-middle, side channel and cryptanalysis approaches. A multi-layer security approach has been acknowledged as an effective and efficient solution for countering security attacks in IoT systems [16]; secure booting using cryptographic hash algorithms and digital signature can increase security in the authentication stage of secure operation in the physical layer. All

devices should authenticate themselves to the network before any data reception or transmission. Point-to-point encryption and authentication mechanisms can be applied to provide security in the network layer [17].

Ronen, Shamir [18] have presented a new and interesting taxonomy of IoT attacks based on how hackers deviate the IoT features. Misusing, reducing, extending and ignoring the system functionality are their approaches to attack IoT devices. They have investigated the functionality of smart lights to show the proof of these concepts. Two attacks were explored in this study: 1) a covert channel was created to capture confidential information from the building of an organisation whose smart lights were connected to the internal sensitive network. An optical receiver read the data from a distance close to the building in order to measure duration and frequency of the changes in the lights intensity. 2) Those lights were used to create strobes in the sensitive light frequency that can cause a risk of epileptic seizures. The results showed that experts should consider all information security aspects in the analysis, design, implementation and integration of the IoT systems.

Attackers are usually experts in this domain and use different approaches to achieve their target[19]. We have explained the most common attacks in the IoT systems to better understand security in IoT. Table 2 shows their definitions, layers that they compromise and their effects on IoT systems.

Table 2

Authentication in IoT

Authentication plays an important role in information security and privacy protection in IoT. Different studies have proposed various approaches to improve authentication in the domain of IoT. A heterogeneous identity-based authentication model, applying the concept of Software Defined Networking (SDN), has been presented by [20]. In this study, SDN has used fog-distributed nodes to overcome resource-restraint; each set of devices has been connected to a gateway that can support authentication. All gateways have been connected to a central controller that has access to central data. A message flows through devices, gateway and controller. Obtaining an authentication certificate from the controller for a gateway, registration to the gateway, and sending a request from IoT devices to the gateway are three basic process in this approach that need enough resources.

Wireless Sensor Networks (WNS) have been discussed in the domain of IoT in many studies. [21] have presented a key establishment scheme in a pervasive authentication protocol in WNS. There are two important stages in this process: 1) users and edge devices should register and obtain cryptographic credentials. 2) A mutual communication with key establishments should be built up in this process. In this protocol, end-users can authenticate themselves to the sensor nodes directly and acquire data and services. The certificates are lightweight and overcome resource-restraint.

The physical state of an object, location and transmission state are characteristics that [22] have used to design a fingerprint for IoT objects in order to authenticate them as an legitimate entity in the system. In this view, various devices have different types of fingerprint features. An object is validated as a legitimate device if the message is sent by a single object. In addition, the Infinite Gaussian Mixture Mode (IGMM) was used to be sure that the fingerprint for each actuator follows a multivariate Gaussian distribution. In the next stage, the result of clustering

by IGMM compare with pattern of device fingerprint. However, the position of an object or fingerprint of an actuator can change due to environmental changes. To overcome this challenge, a transfer learning technique that differentiates normal changes with malicious changes was applied. The results of this study showed improvement in authentication performance, however, these processes need enough computational power, memory, storage and other resources which shows that resource-constraint is still a challenge in this domain.

To overcome the challenge of resource-constraint in an IoT system that negatively influences information security and privacy protection, we have proposed a model that shows how we can choose the resources (actuators in the IoT system) to use maximum capacity in the system for creating fog nodes and improve the quality of services.

Case Study

Research on smart vehicles has attracted the attention of experts in recent years. In many of these studies information security breaches and privacy violation have been mentioned as one of the main concerns that originates from resource-constraint [23,24]. Roadside units (RSUs) [25], cellular network [26,27], mobile cloud computing [28] and fog vehicular computing [29] are examples of solutions that have been presented recently. In this study, we have focused on vehicle fog computing as an effective and efficient approach that can overcome resource restriction in this domain. A significant aspect of this research originates from the inclusion of an approach that helps the system choose the best resources in terms of computation power, memory, storage, most packet delivery, and less power consumption and hop-count in the fog nodes. We have added a decision-making procedure to the decision-making unit that chooses the best alternative node in the fog then finds the other alternative node that has the most similarity (closeness) with the best node.

Fog Vehicle Computing

Cyber preparedness is one of the most important steps in smart vehicle development. HIS Markit has predicted that seventy million connected vehicles will be on the road by 2023 [30]. Collision-avoidance features, autonomous lane changing, self-parking and auto-steering are examples of abilities that current smart cars have. The Internet of Things, computational data analysis, and sensor technologies play major roles in the revolution to produce smarter cars [31]. Future intelligent transportation systems will bring safety, convenience, traffic efficiency, information spreading services (emergency operation for terrorist attacks and natural disasters) and context sharing (entertainment and advertisements). As these new capabilities have been developed, new challenges have emerged that originate from increasing communication and processes that need more computational power. In this research, we have focused on fog vehicle computing (FVC) as one of the efficient solutions due to its advantages:

- FVC is a layer between the edge of the network and cloud; this covers low latency-communication, context awareness, and geo-distribution of smart vehicles.
- FVC empirically can be used in urban environments such as car parks. A pool of smart cars in a shopping centre car park are a valuable resource as supplementary computing, network, memory and storage.
- FVC can cope with emergency situations effectively.

Fog Vehicle Computing Architecture

Physical, fog and cloud layers are three main layers in the vehicle fog computing architecture (Fig 2). Smart cars generate data in the first layer of FVC; different publications use a variety

of names for this layer such as sensing layer, physical layer, perception layer or data generation layer. Smart vehicles produce data that originate from GPS and radar, cameras, etc. These data have been estimated to be about 25 GB per day [29]. Real-time decision-making is vital in this system. The system can transfer the data and process that are used rarely on the cloud and the process and data that are used frequently on the fog to overcome latency and resource-constrained. Fig 2 shows the architecture of FVC in a concise form.

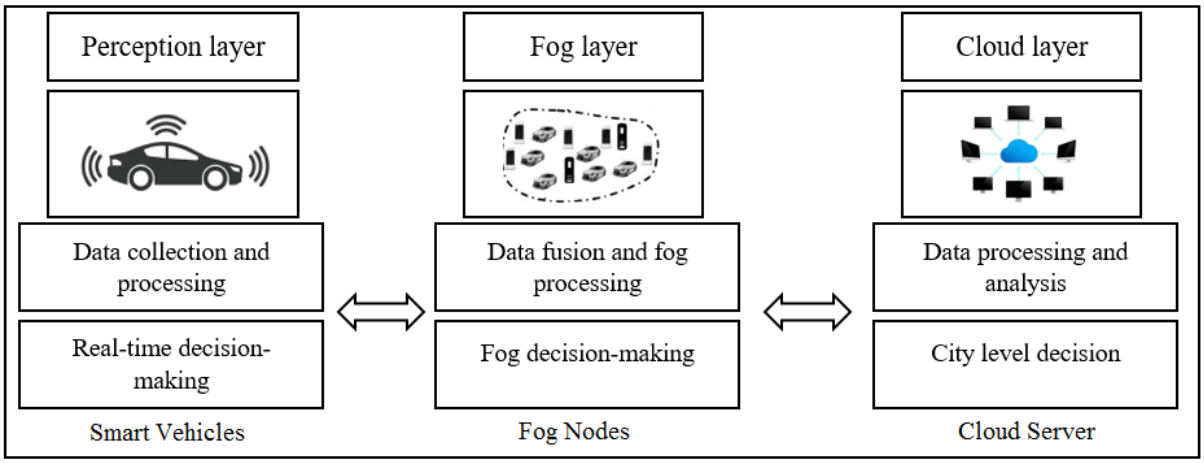

Figure 2: Architecture of Vehicle Fog Computing

Vehicles in car parks, roadside units and nearby can be deployed as nodes in the fog level [32]. Previous studies show that 68% of teenagers surveyed spend more than two hours and 95% of adult shoppers spend one hour at malls every day [33]. Smart vehicles have a certain capacity for data processing, storage and memory. A decision unit in the fog level makes decisions about the transform of process to the fog or cloud. This research endeavours to analyse how the decision-making unit can choose the fog nodes with maximum productivity. We will look at how the decision unit can choose nodes with maximum computational power, storage and memory and nodes that have better connectivity (packet delivery ratio) in the vicinity of the fog (less hop-count). We have defined measurable factors that can help the system to establish the fog nodes, providing maximum resources for the system.

Sookhak, Yu, He, Talebian, Safa, Zhao, Khan, Kumar [5] have proposed a FVC architecture with three main layers:

1) Application and Service Layer
2) Policy Management Layer
3) Abstract Layer

In this model, the Policy Management Layer consists of three sublayers: Policy sublayer, Fog sublayer and Vehicle Cloud sublayer.

The Application and Service layer provides different real-time applications based on the data that have been collected from various sensors or devices such as navigation systems, shopping centre building, parking environment etc. This layer also can provide other services such as Network as a Service (NaaS), Information as a Service (INaaS), Computation as a Service (CaaS), Entertainment as a Service (ENaaS) and Storage as a Service (STaaS).

The Policy Management layer has responsibility for managing tasks by allocating appropriate computation, storage, memory, etc. This layer also responsible for monitoring vehicles, fog, and cloud dynamically.

Policy is the most important layer of the FVC that interconnects with vehicle cloud and fog in order to manage the tasks and resources. All services must be checked by this layer and deliver to the vehicular or fog layers based on the situation and defined policies. In this system, load balancing refers to the maximum number of vehicles, processes, clients and connections that are needed to finish a proposed task. Quality of service is influenced by computational power, network, storage, and memory.

Quality of service (QoS) is based on criteria that relate to network, memory, computing and storage such as delay, computation cost, and communication cost. Configuration determines necessary settings and configuration of various services and devices which are presented or supported by FVC. The set of rules and policies that influence the operation of FVC and help decision-making in terms of security, network requirements and performance are in the *Repository unit*. Different techniques that influence access control, privacy, integrity and availability of information are managed by the *Security and Privacy unit*. The *Service DB* contains the list of processes that are provided by smart vehicles or fog. The *Decision Manager* supports FVC services finder and FVC task manager. The *FVC Service Finder* determines the best service to satisfy the requested service. The *FVC Task Manager* answers this question: whether the assigned task should be fulfilled by fog or cloud in this system based on the time and resources needed to perform the task. Fig 3 shows these sections in the system.

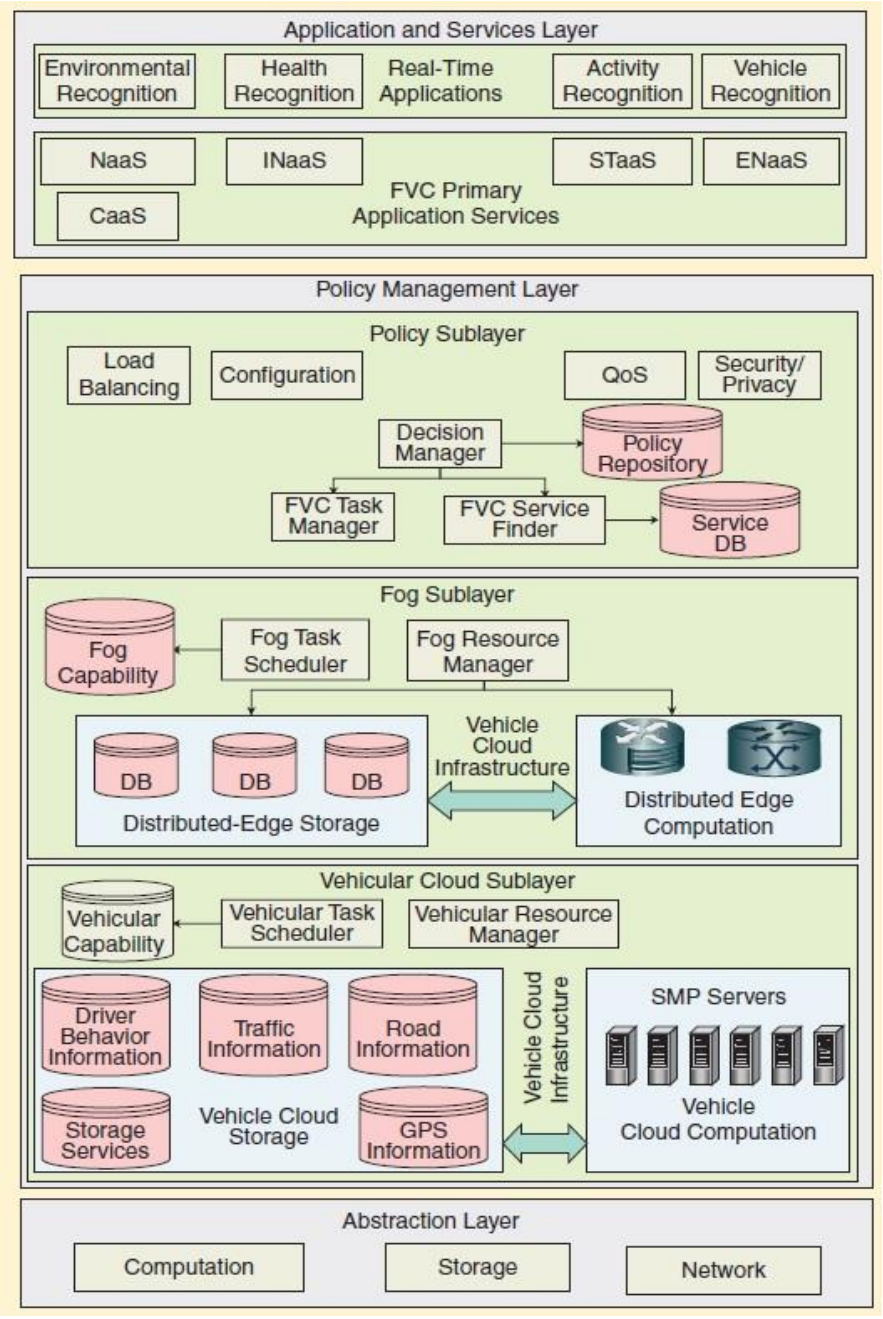

Figure 3: Fog Vehicular Computing Architecture

Fog is another sublayer in policy manager that can serve limited number of requests based on its resources. Fog capability DB contains unassigned fog nodes and their resources to provide various services. *Fog Task Scheduler* investigates the situation of unassigned fog elements to consider suitable nodes in order to fulfil requested services from the fog clusters. *Fog Service Manager* updates the list of fog nodes that they are free. Fog service manager checks the policy repository to identify network configuration and service policies for fulfilling requested services to the free nodes.

The *Vehicular Cloud Sublayer* is another important section in the Policy Management Layer that augments the services that need more computational power. The *Vehicular Capability DB*,

Vehicular Task Scheduler and *Vehicular Resource Manager* are three important parts of this section. The vehicular capability DB contains the list of existing smart vehicular clusters and their resources. The *Vehicular Task Scheduler* assigns the computational tasks to the available vehicles or clusters. The *Vehicular Resource Manager* identifies, manages, and modifies vehicular resources frequently. The *Vehicular Resource Manager* configures networks based on the policies that have been defined in the *Policy Repository*.

The Abstraction Layer provides a homogeneous platform for the FVC and a monotonic interface for monitoring, provisioning and managing the resources such as CPU, storage, memory, network and so on. The Abstraction Layer also controls services on physical machines, hypervisors, and operation systems. This layer has the ability to conduct the visualization technique for supporting multi-tendency and operating systems and services on physical machines for better resource management. Attribute-based cryptography, zero knowledge proof, and homomorphic secret sharing are examples of techniques that positively influence confidentiality, integrity and access control in the FVC system.

This research endeavours to present a model that the FVC can apply to choose the best nodes in order to overcome resource-constraints in the system, besides proposing a common architecture of FVC. The Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) is a multi-attribute decision-making approach through distance measures [34] that helps us to choose the most suitable alternatives to have nodes with maximum resources (computational power, storage, memory and packet delivery) and nodes with minimum power consumption at the vicinity (minimum hop-count) of the edge. To achieve this target, we have defined the below parameters in our system.

Parameters Definition

Positive ideal node is a node that has maximum computational power, storage, packet delivery and minimum power consumption and hop-count in our IoT system.

Negative ideal node is a node that has minimum computational power, storage, memory, packet delivery and maximum power consumption and hop-count in our IoT system.

The computational power (Megahertz) in an actuator is influenced by the memory, speed of processor, size of the register in the CPU, bus type and its speed, and the amount of cache memory.

The storage (Megabyte) is hardware that is used for storing, extracting, and porting data or object, permanently or temporarily.

The memory (Megabyte) in an actuator refers to the device that usually keep data temporally with a random access to the data (RAM). Memory is an integrated part of a computing system.

Packet delivery refers to the ratio of data that is received by a target in a network. In other words, packet delivery is the sum of the data packet received divided by the sum of the data packet that has been produced by the source. This measure shows the quality of the network.

Hop-count refers to the number of steps that data pass from bridges, routers and gateways between source and destination in a network.

This is minimum criteria that we have considered to explain the model. These criteria can be changed based on application of the fog in an IoT system. The significant aspects of this model are derived from the inclusion of:

- Different criteria based on experts' opinion can be applied in the model to maximize productivity of the fog.
- The model has a unified and integrated process that will not increase the computational burden for system.
- Different weight can be considered for every criterion based on the application of fog. For instance, an IoT system such as a wireless sensor network that has a data stream and produces a huge amount of data needs a more storage and less memory; we will consider more weight for storage and less weight for memory in our model.
- We can define the characteristics of the fog by the definition of ideal positive alternative.
- The presented approach can be applied to any type of IoT system such smart homes, smart cities, smart vehicles, etc.

Node Selection Process

The presented model tries to choose the best objects in the IoT system in rank order to overcome resource-constraint. The output of this model is a ranking of objects based on the defined criteria (computational power, storage, memory, etc). In the first step, we need a matrix that contains all objects and their criteria:

We have m objects and n criteria and define smart objects and their criteria as follows:

$$\begin{bmatrix} O_1C_1 & O_1C_2 & \dots & O_1C_n \\ O_2C_1 & O_2C_2 & \dots & O_2C_n \\ . & . & . & . \\ O_mC_1 & O_mC_2 & \dots & O_mC_n \end{bmatrix}$$

We normalise all criteria in order to bring the measure of all criteria below 1. Therefore, the measure of criteria for the object that has the highest measure will be 1 and the lowest measure will be 0. All measures will be between 0 and 1 in our matrix.

R is a normalised matrix with m object and n criteria that all measures are between 0 and 1:

$r_{i,j} = \frac{r_{i,j}}{\sqrt{\sum_{i=1}^{m} r_{i,j}}}$ (if =1, 2, 3,…, m and j=1, 2, 3,…, n)

In this step we can consider the experts' opinion about the importance of criteria, considering weight for them:

$t_{i,j} = r_{i,j} * W_j$ where $W_j = \frac{w_j}{\sqrt{\sum_{j=1}^{n} w_j}}$ j=1, 2, 3, …, n

We have divided the characteristics of an object into positive characteristics and negative characteristics. In this view, positive characteristics should be maximised and negative characteristics should be minimisedfor an ideal positive alternative (object/node). In the same way, the positive characteristics should minimised and negative characteristics should be maximised for ideal negative alternative (object/node).

We define the worst alternative (A_w) and the best alternative (A_b) as follows:

A_w= {(max ($t_{i,j}$|i= 1, 2, …, n| j ε J_-), (min ($t_{i,j}$|i= 1, 2, …, n| j ε J_+)

A_b= {(min ($t_{i,j}$|i= 1, 2, …, n| j ε J_-), (max ($t_{i,j}$|i= 1, 2, …, n| j ε J_+)

Where J_+ = {j=1, 2, …, n|j} are characteristics that have a positive impact
And J_- = {j=1, 2,…n|j} are characteristics that have a negative impact.
In our case, high computational power, packet delivery storage and memory size are positive characteristics that we consider to choose the nodes in our IoT system, and power consumption and hop-count are negative characteristics that should be minimised in our system.

$$d_{i,w}= \sqrt{\sum_{j=1}^{n}(t_{i,j-}\, t_{w,j})^2} \quad , i=1, 2, \ldots, m$$

$$d_{i,b}= \sqrt{\sum_{j=1}^{n}(t_{i,j-}\, t_{b,j})^2} \quad , i=1, 2, \ldots, m$$

Where $d_{i,w}$ and $d_{i,b}$ are characteristics distance between different alternative.

Now, we calculate the similarity between the best and worst condition:

$$S_{i,w}= \frac{d_{i,w}}{(d_{i,w}+ d_{i,b})} \quad , 0 \leq S_{i,w} \leq 1, 2, \ldots., m$$

If $S_{i,w}$ = 1 this means that the selected node is the best node based the criteria that we have chosen, and if $S_{i,w}$ is 0, this means that the selected node is the worst node based on the characteristics that we have chosen. The results show a ranking of nodes based on the characteristics that we have determined.

Experiment

In the simulation process (C# programming), computational cost refers to the time for calculating the algebraic algorithm signature of a file, containing signature generation and integration. Communication cost is defined based on the ratio of successful packet delivery and productivity of the model showing the ratio of completed tasks in comparison with two situations: 1) the nodes are chosen randomly. 2) the nodes are chosen based on the presented algorithm [5].

Table 3

The simulation is based on three main steps:

1) Selection of smart objects based on proposed model and randomly.
2) Calculating the algebraic algorithm signature of a file.
3) Calculating computational cost (Comp-cost), communicational cost (Comm-cost) and productivity of the system.
4) Comparing the results.

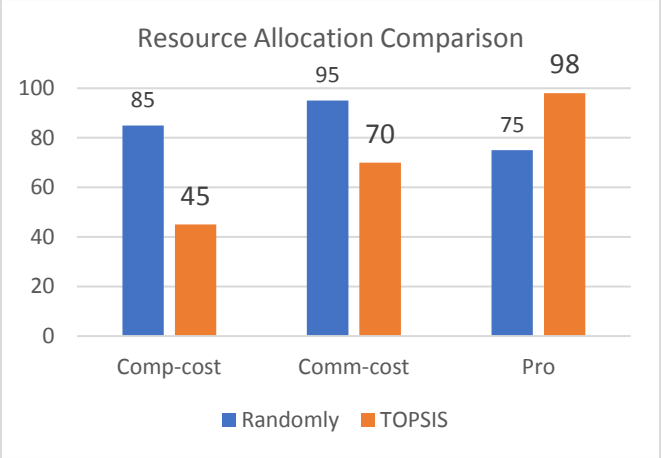

Figure 4: Resource Allocation Comparison

As Table 3 shows we considered 10 smart nodes with maximum five tasks in a restricted environment that we created in our laboratory to test the output of the system. Calculating the algebraic algorithm signature of a file is a time-consuming process that help us to investigate the effectiveness and efficiency of our model. We compared the outputs in two situations - selection of smart objects based on proposed model and randomly. The outputs show that computational cost 20% and communicational cost 25% decrease when the system apply proposed model. The outputs also show that productivity of the system increase 23% when the system use the proposed approach.

Conclusion, Limitation and Future Work

Resource-constraints not only jeopardise information security, but also risk human safety in applications of IoT such as smart vehicles, smart railways, smart traffic control and so on. This research tries to overcome resource-restriction by applying an effective and efficient approach that allows the system to choose the best nodes, create the fog and manage the resources. This approach can be used in every IoT system that several smart objects work in the vicinity of each other. We adopted a multi-criteria decision making (MCDM) model that helps us to select the best nodes to overcome resource-constraint in the fog. We defined computational power, storage, memory, rate of successful packet delivery and hop-count as criteria to choose the best nodes. The outcomes of simulation showed that computational and communicational costs and productivity of the system are better when we use a selection of nodes based on the presented algorithm compared with random selection of nodes.

This study presents several important recommendations besides the proposed approach in order to improve information security in IoT fog systems:

- IoT devices do not have usually malware detection or prevention capability. This should be considered in the security plans.
- IoT systems have the potential of increasing network traffic in specific situations. This negatively influences information security and fog computing can be an effective and efficient approach.
- IoT systems have a dynamic structure; the system should have ability to detect a new legitimate actuator in their vicinity and re-establish the communication after network failures or disruptions.

- Reliable and stable transmission of data is extremely important. The system should be able to decrease the number of transmission errors and provide a good flow of data.
- Resource-constraints such as limited processing power, storage, capacity, memory and bandwidth force the use of a lightweight security approach. Proper application of fog and cloud computing can provide more secure environments in IoT.
- We are faced with a hybrid network in many cases in IoT. Various networks use different protocols. To have a secure environment in our system, we should consider all sections of the network in our security plan.

The proof of concept for this study was not an easy task. We showed the effectiveness of the solution by simulation. But, we had some restrictions in this research; funding restrictions did not allow us to purchase advanced software such as NS2 or NS3, OPNET, COOJA, VEIN, or VSIMRTI in order to test our solution. However, we plan to continue this research and test the presented approach using suitable software. Although we are interested in continuing this research and extending it properly the research project has been defined for one year and this created another limitation.

Artificial Neural Network models can be used for classification and prediction; this research can be continued by focusing on other approaches such as different artificial network models in order to classify the nodes to have the best set of resources in fog computing. We chose smart vehicles in car parks as a case study and showed that based on a selection process computational and communicational costs as well as productivity of the system improve based on a particular selection process. This approach can be used in the other smart environments such as smart traffic control, smart health, and so on and the results can be compared. This research can also be continued by focusing on a solution that considers the resources not only on the fog, but also on the cloud to have better resource management across the entire system. We believe that this research can shed some light for academics and practitioners in this domain.

Acknowledgment

This work has been funded by the UK EPSRC as part of the PETRAS IoT Research Hub.

References

1. Maple C. Security and privacy in the internet of things. *Journal of Cyber Policy.* 2017;2(2):155-184.
2. Safa NS, Maple C, Watson T. An Information Security Risk Management Model for Smart Industries. 15th International Conference on Manufacturing Research ICMR 2017; 2017; London.
3. Yang Y, Wu L, Yin G, Li L, Zhao H. A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal.* 2017;PP(99):1-1.
4. Stojmenovic I, Wen S, Huang X, Luan H. An overview of Fog computing and its security issues. *Concurrency and Computation: Practice and Experience.* 2016;28(10):2991-3005.
5. Sookhak M, Yu FR, He Y, et al. Fog Vehicular Computing: Augmentation of Fog Computing Using Vehicular Cloud Computing. *IEEE Vehicular Technology Magazine.* 2017;12(3):55-64.

6. Alrawais A, Alhothaily A, Hu C, Cheng X. Fog Computing for the Internet of Things: Security and Privacy Issues. *IEEE Internet Computing.* 2017;21(2):34-42.
7. Díaz M, Martín C, Rubio B. State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. *Journal of Network and Computer Applications.* 2016;67(Supplement C):99-117.
8. Mineraud J, Mazhelis O, Su X, Tarkoma S. A gap analysis of Internet-of-Things platforms. *Computer Communications.* 2016;89–90:5-16.
9. Yao H, Bai C, Xiong M, Zeng D, Fu Z. Heterogeneous cloudlet deployment and user-cloudlet association toward cost effective fog computing. *Concurrency and Computation: Practice and Experience.* 2017;29(16):n/a-n/a.
10. Zhang Y, Niyato D, Wang P. Offloading in Mobile Cloudlet Systems with Intermittent Connectivity. *IEEE Transactions on Mobile Computing.* 2015;14(12):2516-2529.
11. Naranjo PGV, Pooranian Z, Shojafar M, Conti M, Buyya R. FOCAN: A Fog-supported smart city network architecture for management of applications in the Internet of Everything environments. *Journal of Parallel and Distributed Computing.* 2018.
12. Zhang W, Lin B, Yin Q, Zhao T. Infrastructure deployment and optimization of fog network based on MicroDC and LRPON integration. *Peer-to-Peer Networking and Applications.* 2017;10(3):579-591.
13. Silva R, Silva JS, Boavida F. Opportunistic fog computing: Feasibility assessment and architectural proposal. Paper presented at: 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM); 8-12 May 2017, 2017.
14. Aazam M, Huh EN. Fog Computing: The Cloud-IoT/IoE Middleware Paradigm. *IEEE Potentials.* 2016;35(3):40-44.
15. Andrea I, Chrysostomou C, Hadjichristofi G. Internet of Things: Security vulnerabilities and challenges. Paper presented at: 2015 IEEE Symposium on Computers and Communication (ISCC); 6-9 July 2015, 2015.
16. Safa NS, Sookhak M, Von Solms R, Furnell S, Ghani NA, Herawan T. Information security conscious care behaviour formation in organizations. *Computers & Security.* 2015;53(0):65-78.
17. Lin J, Yu W, Zhang N, Yang X, Zhang H, Zhao W. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet of Things Journal.* 2017;4(5):1125-1142.
18. Ronen E, Shamir A. Extended Functionality Attacks on IoT Devices: The Case of Smart Lights. Paper presented at: 2016 IEEE European Symposium on Security and Privacy (EuroS&P); 21-24 March 2016, 2016.
19. Safa NS, Maple C, Watson T, Furnell S. Information security collaboration formation in organisations. *IET Information Security.* 2017;12(3):238 - 245. http://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2017.0257.
20. Salman O, Abdallah S, Elhajj IH, Chehab A, Kayssi A. Identity-based authentication scheme for the Internet of Things. Paper presented at: 2016 IEEE Symposium on Computers and Communication (ISCC); 27-30 June 2016, 2016.
21. PawaniPorambage, CorinnaSchmitt, PardeepKumar, AndreiGurtov, MikaYlianttila. PAuthKey: A Pervasive Authentication Protocol and Key Establishment Scheme for Wireless Sensor Networks in Distributed IoT Applications *International Journal of Distributed Sensor Networks* 2014;10(7):1-14.
22. Sharaf-Dabbagh Y, Saad W. On the authentication of devices in the Internet of things. Paper presented at: 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM); 21-24 June 2016, 2016.
23. Bansal P, Kockelman KM, Singh A. Assessing public opinions of and interest in new vehicle technologies: An Austin perspective. *Transportation Research Part C: Emerging Technologies.* 2016;67:1-14.
24. Yu Z, Au MH, Xu Q, Yang R, Han J. Towards leakage-resilient fine-grained access control in fog computing. *Future Generation Computer Systems.* 2018;78, Part 2:763-777.

25. Kuo WH, Tung YS, Fang SH. A node management scheme for R2V connections in RSU-supported Vehicular Adhoc Networks. Paper presented at: 2013 International Conference on Computing, Networking and Communications (ICNC); 28-31 Jan. 2013, 2013.
26. Hampel G, Clarkson KL, Hobby JD, Polakos PA. The tradeoff between coverage and capacity in dynamic optimization of 3G cellular networks. Paper presented at: 2003 IEEE 58th Vehicular Technology Conference. VTC 2003-Fall (IEEE Cat. No.03CH37484); 6-9 Oct. 2003, 2003.
27. Zhioua Gem, Labiod H, Tabbane N, Tabbane S. VANET Inherent Capacity for Offloading Wireless Cellular Infrastructure: An Analytical Study. Paper presented at: 2014 6th International Conference on New Technologies, Mobility and Security (NTMS); March 30 2014-April 2 2014, 2014.
28. He Y, Zhao N, Yin H. Integrated Networking, Caching, and Computing for Connected Vehicles: A Deep Reinforcement Learning Approach. *IEEE Transactions on Vehicular Technology*. 2018;67(1):44-55.
29. Huang C, Lu R, Choo KKR. Vehicular Fog Computing: Architecture, Use Case, and Security and Forensic Challenges. *IEEE Communications Magazine.* 2017;55(11):105-111.
30. Markit I. *The Connected Car.* 2017.
31. LLP FaL. *Connected Cars and Autonomous Vehicles Survey.* 2017.
32. Hou X, Li Y, Chen M, Wu D, Jin D, Chen S. Vehicular Fog Computing: A Viewpoint of Vehicles as the Infrastructures. *IEEE Transactions on Vehicular Technology.* 2016;65(6):3860-3873.
33. *Teen Mall Shopping Attitudes and Usage Survey.* Maryland, USA: Scarborough Research;2009.
34. Yoon KP, Kim WK. The behavioral TOPSIS. *Expert Systems with Applications.* 2017;89:266-272.

Table 1: IoT Architecture Layers

Application Layer Smart home, Smart city, etc.	Interaction with end users or objects
Transport Layer TLS, DTLS, etc.	Reliable transport of data
Network Layer IPsec, 6LoWPAN, etc.	Routing, networking, and topology management
Perception Layer WSN, IMD, RFID, GPS, etc.	Modulation, data collection, signal processing, etc.

Table 2: Common Attacks in IoT Systems

Attack Name	Layer	Description	Effect
Attack on reliability	Application	Inserting a fake node in the IoT network to generate false data or queries.	Creating energy degradation and collisions.
Basic jammers	Perception	Disruption of data transmission by intentional radio emission.	Creating noise and congestion and exhausting the node energy.
Blackhole	Network	Stopping sending data or forwarding the data.	Increasing data loss.
Collision	Data link	Using the occupied radio channel and creating collisions.	Increasing congestion and disrupting the transmission of data.
Data integrity	Transport	Injecting false messages or changing the content of messages.	Falsifying routing data and disrupting the network's normal operation.
Desynchron attack	Transport	Forging messagze between two nodes and losing their synchronization.	Breaking communication links and data transmission.
Denial of Service	Multi-Layer	Making the server and network busy.	Stopping the performance of network.
Eavesdropping	Perception	Hearing and intercepting the data around a node without its knowledge.	Access to private and sensitive information.
Energy drain	Transport	Sending many requests to a node/nodes to establish many connections.	Denial of Service will occur if many nodes affected.
Hardware hacking	Perception	Malicious damage to the nodes.	Losing functionality of nodes.
Hello flood	Network	Broadcasting hello message to entire network with high transmission power.	Collision, energy degradation and false transmission routes.
Intelligent jamming	Data link	Data distribution are known and targeting data packets.	Congestion and exhausting the node energy.
Malicious code attack	Application	Injecting a worm that causes malfunctioning of applications.	Eliminating network's capacity to perform its function.
Man in the middle	Multi-Layer	Intercepting communications between nodes to access key encryption.	Access to sensitive and important network information.
Node tampering	Perception	Physical replacement of a node.	Gaining access to routing table, cryptographic key and other important information.
Replay attack	Network	Repeating a valid data transmission.	Creating traffic, disrupting of routes and creating false error messages.
Selective forwarding	Network	Disallow forwarding messages from selected nodes.	Increasing data loss.
Sinkhole	Network	Distribution of false message to create a centre of attraction for other nodes.	Destruction in transmission routes and increasing data loss.
Spoofed/altered information	Network	Modifying data and creating non-existent information.	Creating routing loops and attracting network traffic.
Sybil attack node replication	Network	Providing multiple identities in the network.	Disorganising transmission routes.
Wormhole	Network	Creating link between fake and malicious nodes in the network.	Undermining cryptography protection and creating false destinations.

Table3: The system configuration

Parameters	Values
Number of fog nodes	10
Number of tasks	1-5
Maximum hop-counts	10
Bandwidth	1024
Network topology	LAN, fully connected