IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 10, No. 1, March 2021, pp. 24~34
ISSN: 2252-8938, DOI: 10.11591/ijai.v10.i1.pp24-34

Deployment of internet of things-based cloudlet-cloud for surveillance operations

Edje E. Abel[1], Abd Latiff Muhammad Shafie[2], Weng Howe Chan[3]
[1,2,3]Department of Computer Science, Universiti Teknologi Malaysia, Malaysia
[1]Department of Computer Science, Delta State University, Nigeria

Article Info

Article history:

Received May 1, 2020
Revised Jan 15, 2021
Accepted Jan 26, 2021

Keywords:

Cloud computing
Cloudlets
Communication protocols
Internet of things
Nation's borders

ABSTRACT

This research proposes the design of internet of things (IoT) camera/toxic gas sensors for the surveillance of a nation's borders. Also, a wearable radio frequency identification (RFID) tag with built-in body-temperature/heartbeat sensors, for monitoring the health status and locations of military personnel while on border patrol duty or in battlefield combats. Mobile micro-controllers are deployed to gather sensed data retrieved from the sensors/RFID tags and transmitted to a cloudlet situated at the command control center, located 200 meters away from the sensor devices. Consequently, sensed data are dispatch to the cloud data center when there is a need for offline data mining or analysis. The distinguishing feature of our proposed system from previous researches is that the health status and locations of troops (soldiers) are monitored while they are in border patrol duty or in battlefield combats. Also, the introduction of cloudlet services closer to the IoT sensor devices for collection of sensed data. This way, the sensed data or information gathered at the cloudlet will aid timely information retrieval that will speed up intelligence gathering for strategic military operations, especially in critical situations. This is an innovative attempt to apply IoT-enabled cloudlet-based cloud computing to support military operations.

Corresponding Author:

Edje E. Abel
Department of Computer Science
Universiti Teknologi Malaysia, Malaysia
Email: eaedje2@graduate.utm.my

1. INTRODUCTION

The survival and safety of any nation depend immensely on the expertise of her military defense. The borders of a nation which is not under consistent surveillance are bound to be compromised by banditry event and influx of illegal migrants. Therefore, it is imperative for the borders to be guarded by innovative technological infrastructural assistive equipment. Consequently, military personnel deployed to physically guard the borders also need to be in good health while performing their civic duty. In any standard border patrol or battlefield environment, there is a military base or command control center that manages the operations and takes decisive decisions of strategizing the reinforcements of border patrol or battlefield combats for an absolute victory over the adversary. Effective and efficient management of military operations at the control center can be achieved with the assistance of software and hardware systems implementation, where internet of things (IoT) sensing devices play a vital role and are integrated with the semantic cloud-based solutions [1]. The word "internet of things (IoT)" was introduced in 1999 by Kevin Ashton. Computers or any digital devices can communicate with each other, share and use information among them without human intervention, aided by IoT. IoT sensing devices are classified as sensors and radio frequency identification (RFID) tags. IoT sensor is a device that captures data from the physical environment and uses built-in compute resource to perform predefined functions upon detection of specific data before passing it on to other devices and network [2]. This was upheld by [3], describing IoT sensor device as any device that collects data and remotely communicate the data to other digital or IoT devices such as controllers and smartphones. Basically, IoT sensors are designed to retrieve a huge amount of data during sensing event of a specific environment. On the other hand, RFID tags are either passive or active, which are used to track down the location of an object. Data obtained from tags are read by the RFID reader, which transmit the data to other devices such as computer systems. However, they are limited in data storage, ubiquitous communication, and computation power as well as architecture technology. Ubiquitous communication requires outstanding innovations, for instance, to support collaborations between things and the internet as well as well-defined connectivity between people and things [4]. Also, IoT sensors need adaptable architecture to enhance the interactivity among diverse transmission structures with various resources for service providers and end user information. On the other hand, cloud computing is a powerful technology to perform massive-scale and complex computing, eliminating the need to maintain expensive computing hardware, dedicated storage space, and software [5]. Consequently, it virtually renders three services namely software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS), on a pay-as-you-go basis.

Integrating IoT devices and the cloud has the potentials to overcome the aforementioned IoT limitations. With the massive data resource storage and computation of the cloud, it is deemed to complement and enhances the performances of IoT devices. Therefore, clients can access the services of IoT devices via the cloud at any time irrespective of their geographical locations. This is due to the fact that cloud offer flexible and scalable assets and requisitions, as well as its services and resources, are timely available and accessible [4]. Therefore, the merging of IoT and Cloud tends to benefits both technologies however there are some challenges that must be overcome before they can actualize their full potentials. The major challenge is the far-reaching communication distance between them. Such long-distance communication results in latency delay and jitter. Latency can give negative impact on interactive response as the task in hand increases, which is not ideal for critical situations in a hostile battlefield environment or border patrol that needs timely intelligent information. Also, it can make render the entire communication systrms unreliable in a military context, especially in the areas of surveillance and intelligence gathering, where timely information is paramount for effective and efficient operations. Therefore, a resource-rich cloudlet computing is introduced to resolve the issue of latency and communication delay between the IoT and the cloud.

Cloudlet is a trusted smaller version of the cloud that comprises clusters of computers that are connected to the internet [6-7]. In addition, it efficiently provides cloud computing services to mobile devices, such as smartphones, tablets, and IoT sensing devices. Cloudlet has the capability to improve the response time applications running on IoT sensing devices by utilizing low latency, high-bandwidth wireless connectivity, as well as hosting the cloud computing resources such as virtual machines, physically closer to the IoT sensing devices accessing them [3]. Thus, eliminate the latency delays of long-distance communication between the IoT sensing devices and the Cloud. The IoT sensing devices function as a thin client, with all its computation performed in the cloudlet. Hence, the proximity of the cloudlet to the IoT is very important for timely (in milliseconds) execution of jobs or tasks in the cloudlet.

To the best of our knowledge, there are limited existing researches on the application of IoT based cloud computing to support military operations at present. For instance, [8] investigate the potential use of IoT in military operations which include risks, network vulnerabilities and the policies governing its utilization. Some of the utilization of IoT highlighted includes the base operational support developed to provide basic support or needs of military personnels and families, and monitoring of military personnel and environment using wearable smart clothing. Consiquently, sisks such as cybersecurity and policy strategy pose challenges for the effective and reliable use of IoT in military operations. In [9], an IoT-base military assistance and surveillance system in the battlefield is developed. Data obtained from the multi-sensor surveillance devices are forwarded to a military unit for the onward process. To transmit the information such as the sensed data and messages that will allow the officers to be updated about the status of the battlefield in real-time as they proceed for combat. Field surveillance robot for land mine detection and toxic gas sensing devices is proposed by [10]. It can detect covered or hidden metals and sensing of toxic gas attacks. The robot is wirelessly controlled by utilizing an android phone. Furthermore, it uses Arduino Uno micro-controller for the gathering of sensed data and NodeMCU WiFi to interface the controller and the robot. Therefore, all sensing information gathered by the controller is transferred to the cloud server and accessed via a designated webpage. Thus, enabling the Robot to be used in real-time at the battlefield and monitored at the military headquarters simultaneously.

The research work of [11] analyzes the applicability of IoT in military defense operations which includes the tracking of object, monitoring the health of military personnel in active service, underground and underwater survulliance as well as predicting the precense of drones. It also highlights how edge technology can be deployed for data gathering in the military domain and how to utilize the data for intillence insight to enhance the defense system capability. The research by [12] investigates the leveraging of IoT within a military network environment, discussing the challenges and solutions. They envisage that challenges such as reconciling the differences between commercial IoT architectural designs and military network architectures, and the realization of efficient resource IoT middleware must be addressed. It also proffers solutions to resolve the aforementioned challenges. In [13] a model-driven engineering (MDE) approach is proposed for the implementation of military health monitoring, to resolve the issue of technological fragmentation between the military settings (e.g., Navy, Air force and army). It also integrates the components and applications deployed by researchers and engineers in various disciplines. The meta-model is achieved by the utilization of IoT devices embedded within the military settings. Consequently, the meta-model resolves the issues associated with the implementation as a product line while enhancing the understanding between engineers and researchers.

The above existing researches have been able to contribute significantly in the deployement of IoT Cloud for military operations. But are unable to address the issue of latency delay between the the IoT sensors and the cloud, to provide timely information needed to facilitate military intelligence gathering in both border surveillance and battlefield operations real time basis. However, [10] utilizes microcontrollers to retrieve sensed data from the robot before been forwared to the cloud, but they are constrained with limited storage capacity and processing power. Microcontrollers are known for their inability to perform multiple numbers of executions simultaneously and unable to interface devices with huge power directly [14-15]. Also, the prevous researches are yet to make provision for the filtering or cleansing of sensory data or signal to remove unusful ones, which is of high importance in military operations so as to obtain relevant information for intelligence gathering. Consequiently, some of the existing researches only focus on health monitoring of military personnel while others pay only attention for detecting hidden exploves or toxic gas in battlefield. Therefore, this research paper tends to deploy cloud enabled cloudlet computing closer to the IoT sensing devices which are distributed in a nation’s borders and perceived enemy territory (environment), for surveillance and monitoring of health status of grand troops while in battlefield combats or border patrol duty. Also, to introduce potential filtering techniques that are capable of removing irrelevant data signal from the overall sensed data signal obtained. The current research contribution is:

- The introduction of a wearable radio frequency identification (RFID) tag with built-in body temperature/heartbeat sensors, for monitoring the health status and locations (where-about) of military personnel in border patrol duty and battlefield combat.
- The deployment of cloudlet close to IoT sensing device(s) to resolve the issues of high latency and delays caused by long-distance communication between IoT devices and the cloud platform.
- The modelling of kalman filtering technique to remove excessive noise or outliers from the data/image(s) captured by the RFIDs/sensors. Thus, to avoid misinformation during military intelligent decision making and wellbeing of military personnel in operations.
- Linear discriminant analysis is formulated to eliminate redundant data/image(s) from the entire captured sensed data in order to obtain relevant data/images needed for intelligent decisions.

The rest of this paper is structured: Section 2 describes the research methodology adopted to actualize the current study. Section 3 provides a detailed insight of the proposed system architecture, for the enhancement of military operations and the health status of grand troops, while in border patrol duty and battlefield combats. Section 4 presents general discussion of the proposed system architecture followed by the challenges for the deployment of IoT-enabled cloudlet-cloud in military contexts, which leads to potential future research directions. Section 5 presnet the concluding remark.

2. RESEARCH METHODOLOGY

We adopted the cyclic action research methodology to conduct this research study. Cyclic action research process enables the generation of prescriptive design knowledge through structuring and evaluating collective Information Technology artifacts in an organizational setting [16]. It is mainly comprised of five stages arranged in cyclical pattern. These stages include assessing the current situation, identify issues from the existing situation, devise a plan to resolve the issues, analyze solution and reflect, as depicted in Figure 1. Therefore, the stages are utilized to actualize the research objectives of this study. Firstly, an investigation was carried out on related existing research works to ascertain the level of utilizing IoT-enabled cloud service to support Military personnel in their operations while on the battlefield in the introductory section of this research. Findings show that there is a significant deployment of IoT-enabled Cloud services to aid the operations of military personnel while on the battlefield with respect to surveillance and access to information. Thereafter, the eminent issues are identified in previous researches (see introduction) that may hinder the effectiveness and efficient use of IoT-enabled cloud services to enhance military operations at the battlefield as well as how it can be extended to support the surveillance of a Nation's border. After which, a plan is devised on how to resolve the issues identified by proposing and formulating IoT-enable cloudlet-cloud architecture model. The proposed system is extensively analyzed as captured in section 3 of this article. Furthermore, we reflect on the propose system capability and discuss some challenges that could lead to potential future research directions in section 4 of this article.

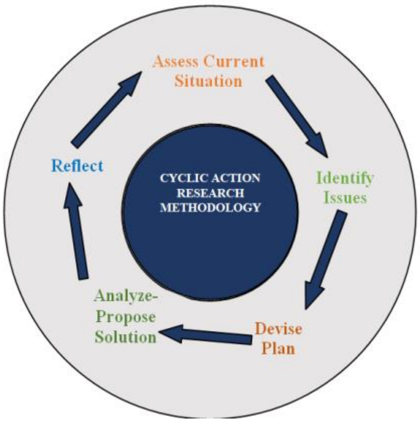

Figure 1. Cyclic action research methodology

3. PROPOSED SYSTEM ARCHITECTURE

The proposed systm model is based on the deployment of camera and toxic gas sensors for the surveillance of battlefield environment and the borders of a nation. As well as a wearable radio frequency identification (RFID) tag with built-in body temperature/heartbeat sensors, for monitoring the health status of grand troops (military personnel) in border patrol and battlefield combat. Consequently, we introduce the services of cloudlet close to the IoT sensing devices and the modeling of a Kalman filtering algorithm, to remove excessive noise or outliers from the data/image(s) captured by the sensors/RFIDs. Furthermore, linear discriminant analysis is formulated to eliminate redundant data and blurred image(s) from the entire sensed information, to obtain relevant data/image(s) needed for intelligent decisions.

IoT camera sensors are attached to multiple drones for monitoring the perceived enermy (advarsory) camp during warfare or the borders of a country to checkmate criminal activities. Also, toxic gas sensors are embedded underground within the battlefield environment. Grand troop soldiers are stationed at proximity to the environment under surveillance, which are also responsible for controlling the drones with a remote-control device(s). Events captured by the sensors are transferred to a controller (Mobile Raspberry), which performs a de-noising process on the sensed data by utilizing a kalman filtering (KF) algorithm. Its major features consist of a 2.4Hz processing speed, 802.11 ac WiFi, dual-band of 2.5GHz and a 1GB RAM. Furthermore, the raspberry Pi is programmed to have a function that communicates directly with the sensors, to either activate or put them in sleep mode. This decision is taken based on the nature of sensing event retrieved from the sensors over duration of time. For instance, if the sensing data from the sensor(s) shows there are no security threat or suspicious event captured over a period of time, sensor(s) are switched to sleep mode so that energy consumption can be minimzed. However, sensors are automatically traggard into active state by a suspicious event such as illegal migrant(s) attempting to cross over the border, group of persons armed with dangerous weapons, and harmful gas aroma detected within the environment. The Kalman filter, named after Rudolph E. Kalman, is often used for smoothing and de-noising of sensing images [17]. It eliminates excessive noise from the sensing signals to obtain the actual ones, by utilizing predictor or a threshold value that is compared with signal sensed data value at an interval. If the sensed data value is greater than the predictor value, then the sensed data is accepted. Sensed data is discarded when its value is less than the predictor value. Algorithm 1 denotes the performance of the KF. Firstly, it assumes the present state P_s is regressed from the previous state P_{s-1}. Therefore, the observation of the present state is depicted as $O_s.Ps|_{s-1}$ which symbolizes the estimation of P at time s, whereas $A_s|_{s-1}$ denotes the estimation accuracy. KF processes the sensed data upon arrival in the raspberry pi due to its recursive functions with minimum usage of memory. The data processing level uses its own ability to infer the optimal estimate from a larger set of data when noise is eliminated from the data by KF. After which valuable data corresponding to the predefined threshold values are generated.

Algorithm 1: Kalman filtering (KF) algorithm

```
1.   $T_s$ – Transition state (Indicating previous state $P_{s-1}$)
     $V_s$ – Variability measurement of the process noise
     $W_s$ – Variability measurement of observing noise
     $R_s$ – Regulate input (indicating the control $vector_s$)
     $U_s$ – Observation process
     $H_s \sim (0, V_s)$
     $N_s \sim (0, W_s)$
2.   Calculating the present state Ps by utilizing the previous state $P_{s-1}$
     $Ps = TsPs-1 + R_sV_s + H_s$
     $O_s = U_sP_s + N_s$
3.   Estimate the present state from the previous state
     $P_s|_{s-1} = T_sP_{s-1}|_{s-1} + R_sV_s$
     Variability measurement prediction
     $A_s|_{s-1} = T_sA_s-1|_{s-1}T_s^T + V_s$
4.   Combining present prediction with present observation
     Present Observation
     $P.O_s = O_s - U_sP_s|_{s-1}$
     Covariance Measurement Observation
     $Vm_s = U_s A_s|_{s-1}U_s^T + W_s$
     Best gain (Actualization of Relevant sensed data)
$Bg_s = A_s|_{s-1}U_s^T Vm_s^{-1}$
```

On the other hand, a radiofrequency identification (RFID) reader with the coverage range of 200m is deployed to read data obtained from both passive and active tags worn by troops (military personnel). The RFID readers are programmed to transmit their information to the raspberry Pi controllers. Hence, sensed data and the information regarding the location of troops are collected in the Raspberry Pi, and then forwarded to the cloudlet via a WiFi communication protocol for onward processing, as depicted in Figure 2.

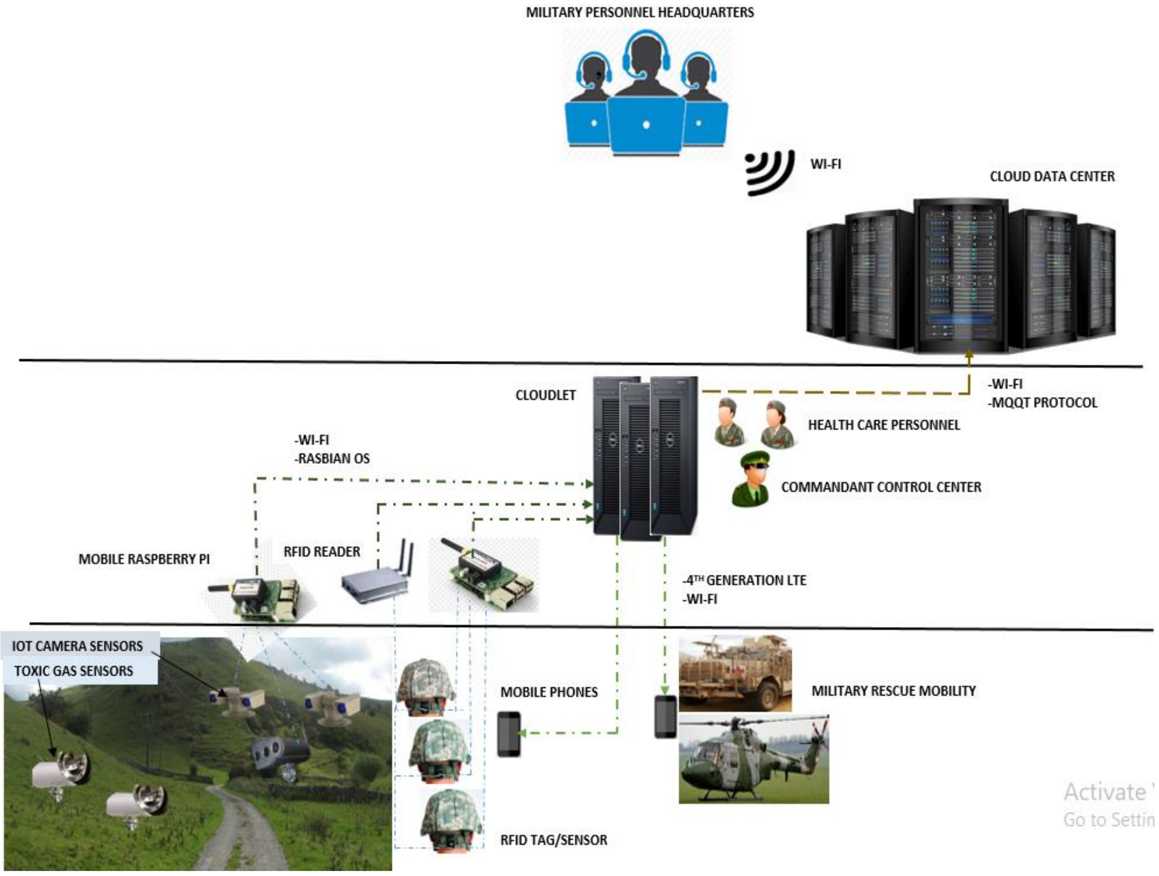

Figure 2. Overview of military assisted IoT-based cloudlet-cloud architecture

Clusters of servers are deployed as cloudlets in close proximity to the IoT devices to reduce the far-reaching distance of the cloud. There is the possibility of sensed data redundant occurrence after the filtering of noise from the sensed data by the KF algorithm. For instance, if camera sensor A captured an enemy and the enemy moves toward sensor camera B, that same enemy will be recaptured by B, resulting to data duplication. Therefore, duplicate sensed data are removed from the filtered sensed dataset to obtain relevant information. The relevant sensed image/data undergoes feature extraction process to obtain the exact image/ data by utilizing a machine learning algorithm. There are three main types of machine learning algorithm namely, supervised, unsupervised and semi-supervised. The supervised learning whose process is majorly classification is well known and mostly deploy for the removal of duplicate sensed data from sensory datasets. On the other hand, the unsupervised which is mainly of clustering process is used for feature extraction. We have adopted the linear discriminant analysis (LDA) algorithm proposed by [18] for the feature extraction process as depicted in algorithm 2. LDA is a powerful classification tool used for both data reduction and feature extraction. Consequently, the relevant sensed data/image undergoes an analytical process in order to obtain meaningful or intelligent information about the status of the environment under surveillance. If the intelligent information obtained shows an enemy within the environment, the grand troop soldiers are alerted via their mobile phones to proceed to the location of the enermy captured within environment (battlefield or border). More so, soldiers are attached with radio frequency identification (RFID) tags fitted with temperature and heartbeat sensors for the monitoring of soldier's location and their health status, while on border patrol duties or combat.

Algorithm 2: Linear discriminant analysis (LDA) algorithm

```
Let $Q_a^TQ_a$ = Non-zeros vectors Matrix, $v_i$ be the ith Non-zero value, V = Non-zero vector, G * J=Matrix diagonal.
Input a set of training captured images {I} where each is known to be N-dimensional vector.
1.  Compute the Non-zero vectors of $Q_a^TQ_a$ with Non-zero values: $N_z = [v_1 \ldots v_r]$, where $r \leq K-1$ and $Q_a$ is from
    $D_{BTW}=Q_aQ_a^T$
2.  Compute the initial r most weighty Non-zero vectors and their corresponding Non-zeros values of the null space of $D_{BTW}$ by $V= Q_aN_z$ and $Aa = V^TD_{BTW}V$ ; Let $M=VA_b^{-1/2}$
    compute non-zero vectors of $M^TD_{SOS}M$, P
3.  Delete (optionally) Non-zero vectors with largest Non-zero values in P. Let $P_G$ and $A_w$ be the G ($\leq r$) selected Non-zero vectors and their corresponding Non-zeros values.
4.  Map all captured images $\{I_i\}$ to the G-dimensional subspace spanned by $⅂ = MP_G A_w^{-1/2}$, and have $\{o_i\}$, where $o = ⅂^TI_i$.
5.  Dimensionality can be reduced further; where the dimensionality of $o_i$ from G to J by executing LDA on {oi}, C(size G * J) be the bases of the Output
6.  Obtain the optimal discriminant feature which is represented by $F = (I) = (⅂W)^TI$.
```

The heartbeat and the body temperature of soldiers are to be monitored as well as their locations on the battlefield or borders in real-time basis. If a soldier is detected of any sudden changes in his health status, the cloudlet immediately relay this information as well as the location of the soldier to the health rescue military team via a mobile phone for quick response. In addition, if a soldier's location is detected to be compromised therefore exposing him to the enemy(s), the military base is alerted via mobile phone for reinforcement. Sensed data are only dispatched to the cloud via WiFi, GPS and message query telemetry transfer (MQTT) protocol, whenever there is no emergency situation or suspected event captured during surveillance operations. However, the available storage space in the cloudlet can be used to cache a portion of the database from the cloud. Thus, to obtain sensed data that has been previously forwarded to the cloud or information send to the cloud via the internet from the military headquarters. For instance, military personnel monitoring the entire event at the force headquarters on the cloud via the internet may decide to ask some troops to pull out from the battlefield and return back home depending on situations on ground. This information can only get to the commandant at the battlefield control center through the cloudlet caching a portion of the cloud database. Furthermore, decisions and communication from headquarters to the battlefield control unit via the cloud is also handled by the cloudlet, which receives such information from the cloud and in turn relay it to the control unit. There are several databases for storing sensed data in cloud platform namely, Hadoop and NoSQL and relational database. The Hadoop and NoSQL database are highly in demand. NoSQL database is known for its provisioning features (such as dynamically modifying data schema, horizontal scalability, memory, and distributed index), which the conventional relational database is unable to provide. On the other hand, Hadoop is an open-source development of Google MapReduce, which supports massive data processing with enhanced performance [19]. Previous researches have proven that the combination of Hadoop and NoSQL databases is an effective means of processing and storing of data, which allows uniform access and, the management data [20]. Figure 3 depicts the general framework of the proposed system illusteraing how the various components of the system interact to each other, followed by a mathematical model of the proposed system framework.

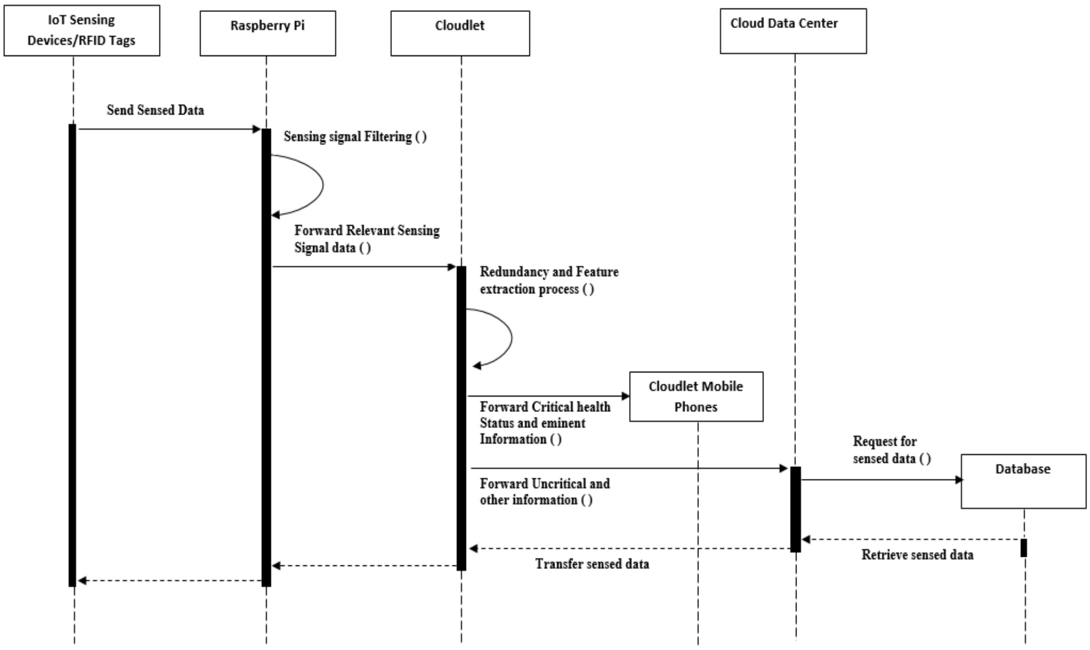
IoT Sensing Devices/RFID Tags
Raspberry Pi
Cloudlet
Cloud Data Center
Send Sensed Data
Sensing signal Filtering ( )
Forward Relevant Sensing Signal data ( )
Redundancy and Feature extraction process ( )
Cloudlet Mobile Phones
Forward Critical health Status and eminent Information ( )
Request for sensed data ( )
Database
Forward Uncritical and other information ( )
Retrieve sensed data
Transfer sensed data

Figure 3. The framework of the military assisted IoT-based cloudlet-cloud

The mathematical model of the proposed system framework as shown in Algorithm 3 is comprise of four main steps. At the initial stage, sensed data genereated from activated sensor nodes are filtered with the support of Kalman Filtering that as shown in Algorithm 1 for the removal of excessive noise (duplicate data). Hence, to obtain relevant sensed data (images), promting the linear discriminant analysis as shown in Algorithm 2 to extract the actual features from the relvant sensed data. The features extracted are used for decisive decision making by the military personnel. As mentioned earlier, sensors are actvitated only when unusual event (i.e. detection of illegal migrants at the boarder an adversary within battlefield) occur, else they remain in an idle state to conserve energy. Furthermore, the functionalty of Algorithm 2 is repeated until all actual features are extracted respectively.

Algorithm 3: Proposed system framework

```
Let T = Sensor node(s)
$A_s$ = Activated Sensor(s)
$I_s$ = De-Activated (Remain in Idle state) sensor(s)
$S_d$ = Sensed data
$R_s$ = Retrieved sensed data
Step1 If Request $S_d$ ==T Then $A_s$
Else $I_s$
Step2 While $R_s$ ; Execute Algorithm 1: Kalman Filtering (KF)
Obtain Relevant sensed Data: $Bg_s = A_s|_{s-1}U_s^T \, Vm_s^{-1}$
Step3 If $Bg_s == A_s|_{s-1}U_s^T \, Vm_s^{-1}$ ;
Call Algorithm 2: Linear Discriminant Analysis (LDA)
Step4: Else If LDA == F (Possible Features) ;
Obtain actual features: $(I) = (\urcorner W)^T I$.
Else Repeat Step4
End IF, End While, End If, End Else If
```

3.1. Network communication protocols deployed

The network communication protocols utilized in our proposed system were carefully selected based on their capabilities to withstand the hazardous nature of the military environment and operations. Message query telemetry transfer (MQTT) protocol is a machine-to-machine application protocol that utilizes the publish/subscribe method for the provisioning of transition flexibility and simplicity of implementation [21]. It can support the smallest monitoring devices such as sensors and has the potential to transmit data over far-reaching devices (Servers or Clients) or intermitted networks. This is actualized by exchanging a series of distinctive control packets, with each control packets having its own purpose. Every bit in the packet is created to minimize the data transmitted over the network. According to [22], MQTT topology has a Server and a client, as both communicate with each other via different control packets. Fourth generation- long-term evolution (4G LTE) is wireless network protocol designed and deployed for the internet protocol (IP) based services such as the combination of multimedia capabilities with applications that require mobile broadband data high-speed transmission rate [23]. It is deemed to be ten times faster than 3G in terms of transmission speed and covers a wider range. Consequently, it's packet core (EPC) and IP-based network framework allows the smooth delivery of voice and data packets as compared to conventional model such as cell tower that utilizes GSM and UMTS. WiFi enables communication between two or more digital devices such as computers and smartphones that are connected to its network. It transmits data over short distances as well as utilizing high frequencies, operating on either 2.4GHz or 5GHz. RFID communication air interface protocol comes in different standards, depending on the type of project it is deployed. However, the 18000-6C and ISO 24730 is deployed in our proposed system. The 18000-6C is an ultra-high frequency which is used for transmitting information from passive tags to the RFID reader [24]. On the other hand, ISO 24730 is deployed to manage the communication of active tags and reader in real-time location. Table 1 shows the characteristics (standard, coverage range, bandwidth, downlink, uplink, frequency band and latency) of the aforementioned network communication protocols discussed.

Table 1. Characteristics of network communication protocols

Protocol	Standard	Range Covrage	Band Width	Down Link	Up Link	Frequency Band	Latency
MQTT	ISO/IEC PRF 20922-OASIS	Wide Range	5-20MHz	256MB	127MB	TCP/IP port 8883	Gigabit Ethernet or Infinite-Band
4G LTE	IEEE 802.16e-2005	Wide Range	1.4MHz to 20MHz	300MGbps	75MGbps	2-8GHz	89.39846ms
Wi-Fi	IEEE 802.11	46m Indoor, 92m Outdoor	20-40MHz	600Mbps	248Mps	2.4GHz	150ms
RFID	UHF RFID-ISO 18000-6C and ISO 24730	Wide Range	2.45MHz	100Kbits/s	-	2.45 and 5.8GHz	10 to 1.5m

4. GENERAL DISCUSSION

The proposed system architecture has the potential of improving military operations based on battlefield warfare and a nation's border suviellance in real time. It has demonstatred timely and reliable intelligence gathering and decision-making process, due to its ability to retrieve, pre-process and the availability of revelant sensed data as at when needed. This was achievedwith the support of cloudlets sited closed to the IoT sensor devices as opposed by previous research work in [10-11]. In [10], they only adopted the use of microcontrollers to retrieve data sensory data from sensors, which are known to be incompatibile with devices of high voltage power, and limited in storage and processing power resource. However, the proposed system utilizes mobile raspberry Pi with sophisticated features that are considered to be robust and reliable for hostile and harzadous border and battlefield environment. Sensory data collected by raspberry pi are futher transmitted to cloudlet where they are formally processed and made available to military personnel for decisive decision making. Thus, leads to the reduction of high latency and delays caused by lon-ditance communication between the IoT devices and the cloud, as opposed to previous research work.

The propose system also outclassed the previous researches such as in [12] by using filtering algorithms firstly, to remove excessive noise or outliers from sensed image/data and secondly, eliminates redundant data/image so as to obtain relevant information. It also monitors the health status of military personel and their locations while in active operations either on border patrol or in warfare, as opposed by previous work in [13] that only consider the health status of grandtroop personel. This was actualized by a wearable RFID tags as discussed in the section above. Monitoring the locations of grandtroops in active services is very important as it provide some significant safety and wellbieng of grandtroops, enabling quick response and assistance when a military personel is ambushed by enemy fire power or his/her health status is below expectation. In terms of communication between the system components-to-components, components-to-military personel and military personel-to-military personel was achieved with the support of selected communication protocols that are presumed to be reliable and efficient, to aid timely interactions and information sharing without interruption during operations.

4.1. Challenges of deployment of IoT-enabled cloudlet-cloud in military contexts

Academic researchers and IT Industries involved in the proliferation of IoT-enabled cloudlet-based cloud for military operations have complex challenges, posed by the hostile and hazardous battlefield/border environment, as well as the strategic nature of military operations. Therefore, there is need to bridge the gap between IT industries and military operational processes to achieve optimal military IoT enabled cloudlet-cloud innovations in the foreseeable future. To this end, a number of IoT-enabled cloudlet-cloud related issues are discussed:

Utilization of network: The availability of network infrastructures in the tactical military operations, are extremely limited by consistent disconnections and radio wave signal fluctuation conditions. These issues often emanate from sensor devices which may drastically disrupt communication leading to loss of vital information. Despite the siting of cloudlet closer to the sensing devices, it is still regarded as an insufficient approach. As long as bandwidth remains the vital resources which the sensing devices depend on for transmitting sensed data to the cloudlet.

Interoperability: Adequate interoperability between devices is often not achievable due to the fact that several functionalities are yet to be served by military hardware and personnel. This issue is usually predominant when there is a need for the integration of device across coalition partners (e.g., between the European Union and African Union). It can be resolved by deploying service-oriented architecture which enables the partners to share information by utilizing a common messaging protocol and distinctive interfaces.

Privacy and security: Failures in military IoT enabled cloudlet-cloud system can compromise the health status of grand troops while in combat and intelligence gathering. Also, military facilities are bound to be subjected to sabotage by the enemies, leading to dissemination of misinformation and service disruption [25].

Utilization of IoT sensors and other devices: Constant power supply to sensors and devices in a border/battlefield environment is another major issue. It is very complicated to supply constant power to sensors and other IoT devices from a stable power source. Also, it is almost infeasible to recharge periodically as in the case of commercial devices. Most IoT devices and sensors are usually powered by a battery source which has a limited lifespan.

Open integration standards: There is an urgent need for IoT ontologies to be integrated with existing standards in order to ensure interoperability among devices with different functionality and ownership [26]. However, ontology-based reasoning as initially been applied to military sensor management systems such as pairing sensors to mission tasks.

5. CONCLUSION

In conclusion, this paper has discussed the deployment of IoT sensors/RFID tags enabled cloudlet cloud computing for the surveillance of a nation’s border or battlefield environment. The proposed system consists of a cloudlet that reduces the latency and delay of transmitting sensory data from IoT sensors to the cloud. This leads to the provision of timely information for intelligence gathering, as opposed to previous researches in this field. Therefore, the integration of IoT sensing devices and cloudlet-based cloud computing holds future promises and opportunities to explore, in terms of researches and investment profit returns. It is also made up of filtering algorithms that were used to remove noise or outleirs and redundant data from sensed data sample, so that relevant data can be retained. Furthermore, the health status and the locations (where-about) of military personel in active services, based on border patrol or in battlefield are monitored in real time as opposed by previous researches. We also introudeced some network protocols to aid interaction between the system components and military personel. In the future, we intend to implement and text run our proposed model in real life scenario to aid the management of sensed data retrieved from sensors with respect to de-noising and the removal of redundant sensing image via feature extraction technique.

ACKNOWLEDGEMENTS

Special thanks to Dr. Alade Abel, for his support and contributions. This work also supported by the Trans Disciplinary Research Grant from Universiti Teknologi Malaysia (grant number: 07G17).

REFERENCES

[1] D. Singh, *et al*., “A survey of Internet-of-Things: Future Vision, architecture challenges and services,” *World Forum on the Internet of Things (WF-IoT) IEEE*, pp.287-292, 2014, doi: 10.1109/WF-IoT.2014.6803174.

[2] M. Rouse, "Internet of Things*," Tech Target-IoT Agenda*, pp. 2-8, 2016, https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

[3] E. A. Fischer, "The Internet of Things: Frequently Asked Questions," *Congressional Research Service Workshop*, pp. 1-4, 2015.

[4] Ali, Afiq & Ahmad, Nazrul & Muhamad Amin, Anang Hudaya, "Cloudlet-based cyber foraging framework for distributed video surveillance provisioning," *2014 4th World Congress on Information and Communication Technologies, WICT 2014*, pp. 199-204, 2015, 10.1109/WICT.2014.7076905.

[5] I. A. T. Hashem *et al*., "The rise of Big Data on Cloud Computing: Review and Open Research Issues,*" Information Systems (Elsevier)*, vol. 47, pp.98-115, 2015, https://doi.org/10.1016/j.is.2014.07.006.

[6] M. Satyanarahanan *et al*., "The Case for VM-Based Cloudlets in Mobile Computing," *Pervasive Computing (IEEE)*, vol. 8, no. 4, pp.14-23, 2009, doi: 10.1109/MPRV.2009.82.

[7] Y. Jararweh, L. Tawalbeh, F. Ababneh and F. Dosari, "Resource Efficient Mobile Computing Using Cloudlet Infrastructure," *2013 IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks*, Dalian, pp. 373-377, 2013, doi: 10.1109/MSN.2013.75.

[8] Mary E. Herman, "Military Applications for the Internet of Things," *A Capstone Project Submitted to the Faculty of Utica College*, pp. 1-48, 2019, https://search.proquest.com/docview/2316439633?pq-origsite=gscholar&fromopenview=true.

[9] R. P. and S. Bagwari, "IoT Based Military Assistance and Surveillance," *2018 International Conference on Intelligent Circuits and Systems (ICICS)*, Phagwara, pp. 340-344, 2018, doi: 10.1109/ICICS.2018.00076.

[10] M. Ashokkumar and T. Thirrumurugan, "Integrated IoT based Design and Android operated Multi-purpose Field Surveillance Robot for Military Use," *International Conference for Phoenixes on Emerging Current Trends in Engineering and Management (PECTEAM*), *Advances in Engineering Research (AER) Journal (Atlantis Press),* vol. 142, pp. 236-243, 2018, https://doi.org/10.2991/pecteam-18.2018.42.

[11] L. Mishra, Vikash and S. Varma, "Internet of Things for Military Applications," *2020 7th International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, pp. 118-123, 2020, doi: 10.23919/INDIACom49435.2020.9083730.

[12] M. Tortonsesi *et al*., "Leveraging Internet of Things within the Military Network Environment-Challenges and Solutions," *World Forum on the Internet of Things (WF-IoT). Third Annual IEEE*, pp. 111-116, 2016, doi: 10.1109/WF-IoT.2016.7845503.

[13] R. P. Reyes Ch., H. P. Vaca, M. P. Calderón, L. Montoya and W. G. Aguilar, "MilNova: An approach to the IoT solution based on model-driven engineering for the military health monitoring," *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*, Pucon, pp. 1-5, 2017, doi: 10.1109/CHILECON.2017.8229585.

[14] C. Schuss and T. Rahkonen, "Use of mobile phones as microcontrollers for control applications such as maximum power point tracking (MPPT)," *2012 16th IEEE Mediterranean Electrotechnical Conference*, Yasmine Hammamet, pp. 792-795, 2012, doi: 10.1109/MELCON.2012.6196549.

[15] M. Graube, S. Hensel, C. Iatrou and L. Urbas, "Information models in OPC UA and their advantages and disadvantages," *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, Limassol, pp. 1-8, 2017, doi: 10.1109/ETFA.2017.8247691.

[16] M. K. Sein *et al*., "Action Research Design," *MIS Quarterly*, vol. 35, no. 1, pp. 37-56, 2011.

[17] J. Pan, *et al*., "Image noise smoothing using a modified Kalman filter," *Neurocomputing (Elsevier)*, vol. 127, pp.1625-1629, 2016, https://doi.org/10.1016/j.neucom.2015.09.034.

[18] Juwei Lu, K. N. Plataniotis and A. N. Venetsanopoulos, "Face recognition using LDA-based algorithms," in *IEEE Transactions on Neural Networks*, vol. 14, no. 1, pp. 195-200, Jan. 2003, doi: 10.1109/TNN.2002.806647.

[19] K. Shvachko, H. Kuang, S. Radia and R. Chansler, "The Hadoop Distributed File System," *2010 IEEE 26th Symposium on Mass Storage Systems and Technologies (MSST)*, Incline Village, NV, pp. 1-10, 2010, doi: 10.1109/MSST.2010.5496972.

[20] Y. Xu, *et al*., "Integrating Hadoop and Parallel DBMs," *Proceedings of the ACM SIGMOD International Conference on Management of data*, pp. 969-974, 2010, https://doi.org/10.1145/1807167.1807272.

[21] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, Fourthquarter 2015, doi: 10.1109/COMST.2015.2444095.

[22] Micheal Yuan, "Getting to Know MQTT", *IBM Community*, pp.1-3, 2014, https://developer.ibm.com/technologies/messaging/articles/iot-mqtt-why-good-for-iot/.

[23] E. Dahlman *et al*., "4G LTE/LTE-Advanced for Mobile Broadband", *Technology and Engineering-Academic Press*, pp. 9-10, 2013.

[24] M. Roberti, "What Protocols Are Used to Communicate Between An RFID Reader and Tag*?," RFID Journals*, pp. 1-11, 2019, https://www.rfidjournal.com/question/what-protocols-are-used-to-communicate-between-an-rfid-reader-and-a-tag.

[25] Don Snyder *et al*., "Improving the Cyber-security of U.S Air Force Military Systems throughout Their Life Cycles," *RAND Corporation*, pp. 1-9, 2015.

[26] S. Staab *et al*., "Knowledge Processes and Meta Processes in Ontology-Based Knowledge Management," *Handbook on Knowledge Management*, pp. 47-67, 2013, DOI: 10.1007/978-3-540-24748-7_3.

BIOGRAPHIES OF AUTHORS

Edje Efetobor Abel (Corresponding Author) is currently a Ph.D. scholar at the School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia. He obtained his MSc (Information Systems Management) in 2010 and BSc (Network Computing) in 2009, in Brunel University, West London, United Kingdom. His area of interest is Cloud Internet of Things, Grid Computing, Network Computing, and Information Systems Management. Also, he is lecturing at Delta State University, Abraka Campus, Nigeria.

Muhammad Shafie Bin ABD Latiff received his Ph.D. degree in 2000 from Bradford University, United Kingdom. He is a Professor and currently the Head of Pervasive Computing Research Group at the School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia (UTM). His research interests are in computer networks with the focus generally on routing protocol, grid, and cloud computing and wireless sensor networks.

Chan Weng Howe received his Bachelor of Computing Science in Bioinformatics and Ph.D. in Computer Science from Universiti Teknologi Malaysia in 2011 and 2016 respectively. He is an active Senior lecturer in the Universiti Teknologi and its main research interests are computational intelligence, bioinformatics, and IoT for healthcare.