Sustainable Cities and Society 59 (2020) 102220

Contents lists available at ScienceDirect

Sustainable Cities and Society

journal homepage: www.elsevier.com/locate/scs

Blockchain and federated learning-based distributed computing defence framework for sustainable society

Pradip Kumar Sharma[a], Jong Hyuk Park[b,*], Kyungeun Cho[a,**]

[a] Department of Multimedia Engineering, Dongguk University, Seoul, 04620, South Korea
[b] Department Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul, 01811, South Korea

ARTICLE INFO

Keywords:
Distributed computing
Internet of battle things
Sustainable society
Blockchain
Federated learning

ABSTRACT

Ensuring social security through the defense organization determines the creation of links between the army and society. Realizing the benefits of the Internet of Battle Things in the defense system can perfectly monetize intelligence and strengthen the armed forces. It establishes a network for strong connectivity in the army with good coordination between complex processes to effectively edge out the enemies. However, this new technology poses organizational and national security challenges that present both opportunities and obstacles. The current framework of the defense IoT network for sustainable society is not adequate enough to make actionable situational awareness decisions in order to infer the state of the battlefield while preserving the privacy of sensitive data. In this paper, we propose a distributed computing defence framework for sustainable society using the features of blockchain technology and federated learning. The proposed model presents an algorithm to meet the challenges of limited training data in order to obtain high accuracy and avoid a reason specific model. To evaluate the effectiveness of the proposed model, we prepare the dataset and investigate the performance of our framework in various scenarios. The result outcomes are promising in terms of accuracy and loss compared to baseline approach.

1. Introduction

To build a sustainable society, the task of ensuring social security through the defense organization determines the creation of links between the army, society and state institutions in the environmental, economic and social fields. Military organizations operating in the public arena are somehow involved in the challenges of local social communities, cooperating with them in crisis situations in different contexts. Defense organizations are beginning to wonder when and how to integrate increasingly autonomous things into their operations in order to ensure the safety and efficiency of civilians in society. The defense system should be smart and efficient enough to keep people safe in order to build a sustainable society, just as private organizations use automation to reduce workplace injuries and ensure error-free production. In all countries, the defense army is the hidden treasure of the nations who work day and night with the latest weapons to fight on the battlefield without worrying about their lives. To edge out the enemies effectively and efficiently, the armed forces must adopt the advantages of emerging technologies like high connectivity network to obtain real-time information and know the situation on the battlefields. Recently, the trend of Internet of Battle Things (IoBT) has a growing utility in defense (Suri et al., 2016). By deploying the smart devices and sensors in various combat or conflict zones, defence intelligence makes it possible to gather precise information on situations in real time to command and control the systems adequately. A recent survey predicts that by 2023, the defense IoT market will reach $ 40,950 million with a Compound Annual Growth Rate (CAGR) of 11.8 % (Nieto & Rios, 2019). To facilitate soldiers' health monitoring, equipment maintenance, inventory management, etc., the IoBT in defence market integrates various tools and services. For a sustainable society, we have to conduct more effective field operations with better situational awareness by army commanders and need to deploy millions of sensors and smart devices.

However, the IoBT represents a new source of exposure in the society, and national defense authorities are concerned about their country's exposure to attack. The rapid increase in the use of IoBT in the society raises a red flag for many defense and government organizations. The use of IoBT devices such as drones, wearable devices, ground

* Corresponding author at: Department of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech), 232 Gongneung-ro, Nowon-gu, Seoul, 01811, South Korea.
** Corresponding author at: Dept. of Multimedia Engineering, College of Engineering, Dongguk University 30, Pildong-ro 1-gil, Jung-gu, Seoul, 04620, South Korea.
E-mail addresses: pradip@dongguk.edu (P.K. Sharma), jhpark1@seoultech.ac.kr (J.H. Park), cke@dongguk.edu (K. Cho).

https://doi.org/10.1016/j.scs.2020.102220
Received 25 March 2020; Received in revised form 20 April 2020; Accepted 20 April 2020
Available online 11 May 2020

sensors, etc., is increasing and the secure distributed computing defence framework for a sustainable society has so far lagged behind deployment (Defense Policy & the Internet of Things Disrupting Global Cyber Defenses, 2019; IoT In Aerospace & Defense Market, 2019; Mohammadi, Rahmani, Darwesh, & Sahafi, 2019). The absence of a secure framework makes defense organizations vulnerable to both internal misuse and hacking. Imminent work in this area to provide the defense IoT should in particular focus on the provision of secure connections via suitable topologies. In addition, in order to make actionable situational awareness decisions to infer the state of the battlefield, the self-organized, resilient, autonomous, on-device computing of the distributed fusion of heterogeneous local data network infrastructure is required (Farooq & Zhu, 2017; Jalaian, Koppel, Harrison, Michaelis, & Russell, 2018; Kott, 2018; Lee, Kim, & Lee, 2019; Lin, Xia, Li, Wang, & Humar, 2019).

Nowadays, the rapid adoption of blockchain technology described as a collaborative ecosystem that has the potential to solve the trust issues between all parties involved in building sustainable smart cities. It helps the population to meet the challenges of urbanization via better implementation of the smart cities framework (Ren, Liu, Ji, Sangaiah, & Wang, 2018, 2020; Sharma, Kumar, & Park, 2020; Xia, Tan et al., 2019). Most organizations in various sectors have started to integrate blockchain technology to advance urban planning, reconsider their current energy and transport management and develop a new business planning framework. Some researchers have introduced blockchain technology to coordinate, integrate and control different urban services with transparency, efficiency, security and privacy (He et al., 2017; Ren et al., 2018; Ren, Leng, Wang, & Kim, 2019).

In this article, we vision the integration of emerging cutting-edge techniques such as blockchain technology and federated learning has potential to address the limitations of current IoBT network architecture and build a distributed computing defence framework for the sustainable society. The scientific contribution of this research work is as follows:

- We propose a multi-layer distributed computing defence framework for sustainable society by leverage the features of blockchain technology and federated learning.
- The proposed model introduces an approach to address the limitation of limited training data at local nodes and train the model based on global view of the defence IoT network with perversion of data privacy.
- We also presents the structure of block in the blockchain network with detail computing workflow at multiple layers.
- To evaluate the proposed model, we prepare the dataset for an experiment on classifying images using federated learning and investigate the performance of our framework in various scenarios.

The rest of the article is structured as follows: Section 2 discuss the issues of adopting IoBT, role of distributed computing in IoBT, and how we can leverage the strength of blockchain technology and federated learning in defence IoT; We present the design overview of the proposed distributed computing framework, methodology, and detail computing workflow in Section 3; Section 4 presents the performance of the proposed computing model in different scenarios; Finally, Section 5 presents the conclusion of this work.

2. Preliminaries

2.1. Importance of defence system for a sustainable society

On the basis of several factors directly/indirectly, the intensity of the defense organization is linked to social communities, in particular in the economic and social aspects in the context of sustainable development. Sirko, Kozuba, and Piotrowska-Trybull (2019) identified and characterized the links of military units in the context of sustainable development. They presented the attributes in social environments to assess the links of opinion of residents, local authorities and soldiers. Smaliukiene (2018) recognized the significant development of the literature on sustainability issues in the military and presented the systematic review of the literature on social cohesion, environmentally sustainable solutions and the economic sustainability of militarization. In the field of sustainability in the defence system, they concluded that social sustainability is currently the dominant area of research. The lack of automation of the defense system, the weakness of the internal security forces, the remains of the military and war security apparatus pose great risks for internal security in post-conflict societies. Meanwhile, advanced technologies such as blockchain technology have drawn considerable attention in various fields to build a sustainable society ecosystem. Khan, Asif, Ahmad, Alharbi, and Aljuaid (2020) presented the different aspects of blockchain technology to improve security issues in the societies for sustainable development. Lever & Kifayat (2020) argued that privacy and security are the primary requirement; and identifying and mitigating security risks is essential to building a robust computing network for a sustainable ecosystem. Some other researchers have also stressed the importance of responding to cybersecurity concerns in the computing network architecture to build the ecosystem of sustainable society (Ande, Adebisi, Hammoudeh, & Saleem, 2019; Laufs, Borrion, & Bradford, 2020; Wang, Yang, Wang, Sherratt, & Zhang, 2020; Xia, Fang, Zou, Wang, & Sangaiah, 2019). Based on the literature review, we can state that the link between defense system and sustainable society and the way security and privacy issues play an important role in building an ecosystem of sustainable society.

2.2. Adoption of internet of battle things (IoBT)

The adaptation of IoBT is the realization of ubiquitous computing, sensing, and monitoring where everything will be a smart device and potentially a processor where subsequent information is on a scale never seen before. Army commanders have always lived and died of information, but the adaptation of the IoBT allows to have a very large and dense number of smart devices to help to eliminate common concerns about the availability of any of them at any given time. However, potential threats to privacy can be compromise crowdsensing services. These new technologies poses organizational, security and privacy challenges that present both opportunities and obstacles. This can lead to sharing of sensing data between devices/organizations combined with robust short range communications, which poses privacy concerns. Due to the high sensitivity of the data, most organizations do not want to share with intermediaries or servers. But, we need to train the model to enable validation, interpretation, fusion and assessment of the reliability of information while preserving the confidentiality and security of local data. To capture the resulting knowledge, a machine-

interpretable, formal, widely applicable and military-relevant language will be necessary to express the information needs in a very heterogeneous IoBT (Kott, Swami, & West, 2016; Russell & Abdelzaher, 2018; Tosh, Shetty, Foytik, Njilla, & Kamhoua, 2018).

2.3. Distributed computing in IoBT

In the military organizations, the distributed computing combat platform is highly needed to allow information and control to go further when appropriate, providing operational flexibility to deal with a near peer targeting the national data systems (The Internet of Things for Defense, 2019). In addition, the distributed computing combat platform also refers to the idea of continuing to operate in the event of failure of one or more nodes and the information that system processes are still available to the battle commander. Adapting the IoBT can facilitate the acquisition of a perfect knowledge of the situation and the control of various conflict zones or battle zones. We need a computing framework to become self-aware and have the intelligence to discover and characterize new components on the battlefield without compromising data confidentiality (Abdelzaher et al., 2018b).

In general, distributed learning is one of the preferable approach to learning activities and allows learners and instructors to participate in learning activities for disparate locations. However, in the context of IoBT, existing distributed learning systems have several limitations (Abdelzaher et al., 2018a). The IoBT consists of a heterogeneous mixture of sensing and computing nodes with different capacities and resources, in which distributed learning is not a good match for training models. On the other hand, federated learning compliments the limitations distributed learning specifically in the context of IoBT. In particular, federated learning aims to train the model on heterogeneous datasets located in various local nodes. Unlike distributed learning focused on training the model on multiple servers with almost same size datasets distributed identically, federated learning is capable of training the model on the datasets are generally heterogeneous and their sizes can span several orders of magnitude (Konečný et al., 2016).

2.4. Integration of Blockchain and federated learning

In the conventional federating learning model, it relies on the single aggregation node to perform the aggregation of the model and the update to the local nodes. First of all, it raises the concern of single point failure, in the case of aggregator node malfunction and compromised due to cyber-attack. Second, it does not rewards the local nodes for their participation in the training model process. The local node with large local dataset leads to their cost in terms of resources and energy during the training of global model. Blockchain technology has potential to provide a secure platform to enable the on-device federated learning in defence IoT network. Some researchers have viewed Blockchain technology as an appropriate platform for building the distributed computing framework using federated learning (Rathore, Kwon, & Park, 2019; Singh, Rathore, & Park, 2019). Kim, Park, Bennis, and Kim (2019) proposed on-device machine learning using Blockchain consensus features without the need of centralized training data. By considering the consensus, computation, and communication delays, the analyzed the latency delay and characterization of the optimal block generation rate. For distributed multiple parties, another secure data sharing architecture using Blockchain and federated learning is proposed by Lu, Huang, Dai, Maharjan, and Zhang (2019). Yang, Liu, Chen, and Tong (2019) also discussed the potential of integration blockchain technology and federated learning to solve data sharing problems between industries so that they can work together to achieve optimal results.

3. Proposed distributed computing defence framework

As we discussed in the previous sections, for the information generated by the IoBT to be useful, without compromising the security and privacy of the data, and in order to minimize the enemy's chances of acquiring information, a robust computing framework for the defense IoT is needed. In this section, we discuss the overview of the design of the proposed distributed computing defence framework for a sustainable society, methodology, and its workflow.

3.1. Design overview

Fig. 1 presents an abstract overview of the proposed distributed computing defence framework for a sustainable society. The proposed model is divided into four different layers: data layer, edge layer, fog layer, and cloud layer. The data layer contains actual local training data collected from surrounding environments. It also includes the different organizations that work at ground level and have sensitive data that they do not want to share with other organizations, agencies, intermediaries, etc. These data are very vital to train model to make decisions with high accuracy rate. The proposed model provides the features to train the model so that it can make a decision with great accuracy, based on local training data, without sharing with intermediaries.

The edge layer consists of several edge nodes connected using Blockchain. Each edge node has several minor nodes to validate the transaction when creating a new block. Each edge node has its own off-chain Blockchain to store the temporary training model while generating an aggregate model using federated learning. In addition, the fog node in the fog layer is also connected using Blockchain to generate a trained model based on a wide range of local training data at the data layer level. The Fog node also includes the number of minor node to validate each aggregate model using federated learning and store the temporarily formed model in its own off-chain. At the cloud layer, the framework generates the global model train based on the selected data available at the edge of the network. We discuss the detailed methodology and workflow of the proposed distributed computing framework in the following subsections.

3.2. Methodology of computing model

Majority of the data generates at the edge of the network and the privacy-sensitive nature of the data owing by devices/organizations/agencies at the data layer, we are not allowed to directly share the data with intermediaries/servers especially in defence IoT. In this proposed model, instead of sharing the actual data, the data

Algorithm 1: Distributed Computing Model Algorithm

Input
ω_i, ρ_i of $d_i, \forall\ i = 1, 2, \ldots, n$
Proxy model $EM_e(t), FM_f(t), and\ CM_c(t)$, where $t \leftarrow 0$

Begin

Phase I: Edge Layer
For $t_e = 0, 1, \ldots, T-1$ Do
Edge nodes broadcast $EM_e(t)$ to all d_i
SharedParameter $d(\omega_i, \rho_i) \leftarrow TrainModel\ (LocalData_i)$
$AggModel\ (EM_e(t))$
If (Validate $(EM_e(t))$)
Add_OffChain $\leftarrow EM_e(t)$
If (Validate $EM_e(t)$) at Peer Edge Nodes
Add_Blockchain $(EM_e(t))$
Broadcast $EM_e(t)$

Phase II: Fog Layer
For $t_f = 0, 1, \ldots, T-1$ Do
Fog nodes broadcast $FM_f(t)$ to lower layer nodes
If (Type is True)
SharedParameter $d(\omega_i, \rho_i) \leftarrow TrainModel\ (LocalData_i)$
$AggModel(AggModel\ (EM_e(t)))$
If (Validate $(FM_f(t))$)
Add_OffChain $\leftarrow FM_f(t)$
If (Validate $FM_f(t)$) at Peer Fog Nodes
Add_Blockchain $(FM_f(t))$
Broadcast $FM_f(t)$

Phase III: Cloud Layer
Repeat the Phase I and II to generate global model

End

layer will only share the model parameter based on the local training data. Intermediaries such as edge node, fog node, etc. will only receive the aggregate of parameters sent by the data layer using the federated learning technique.

Suppose, we have d devices/organizations/agencies at the data layer that have their own privacy-sensitive local data. Each of them containing model parameters ω_i and ρ_i, the aggregate parameter at the intermediary node is computed as $\sum_{i=1}^{d} \omega_i \rho_i / \sum_{i=1}^{d} \rho_i$. Since each derive/organization/agency in defence IoT at data layer will have limited training data, the accuracy of the trained model will not be high and will be region specific. To overcome this limitation and train the model based on global view of the defence IoT network, this model proposed the algorithm 1.

The algorithm I comprises of three phases: edge, fog, cloud layers. In

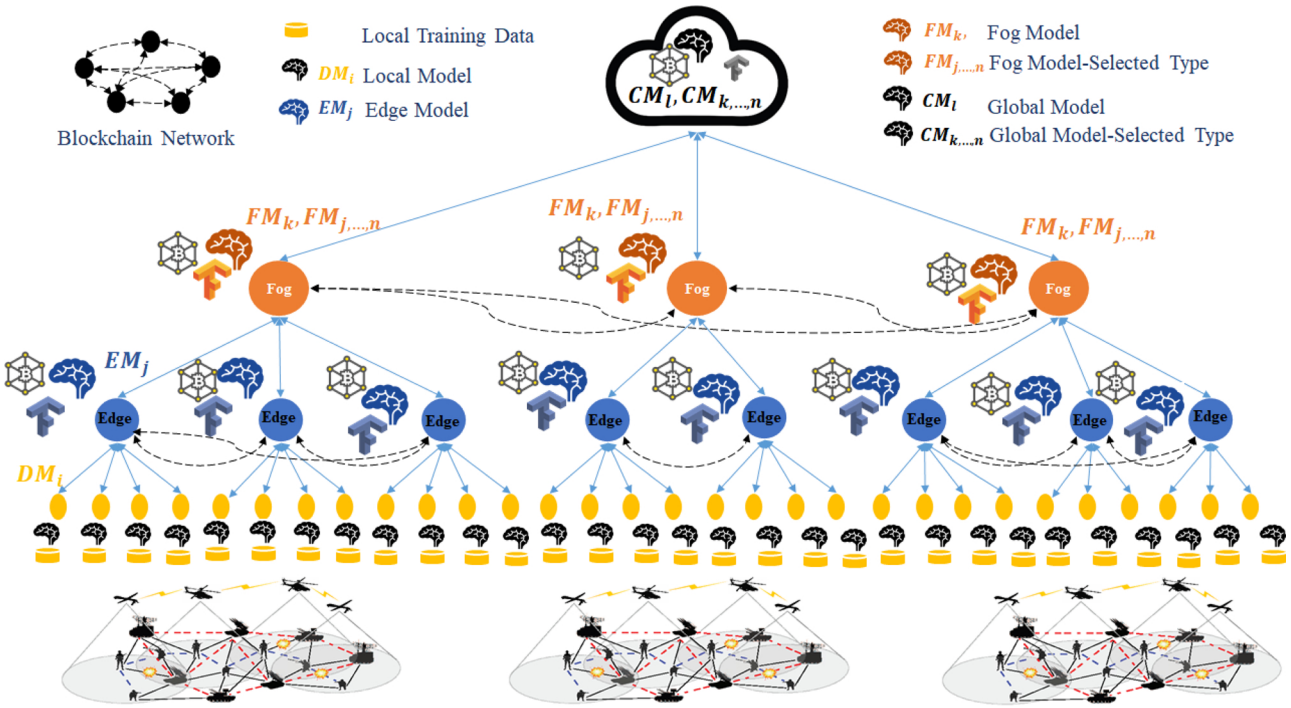


Fig. 1. An abstract overview of the distributed computing defence framework for sustainable society.

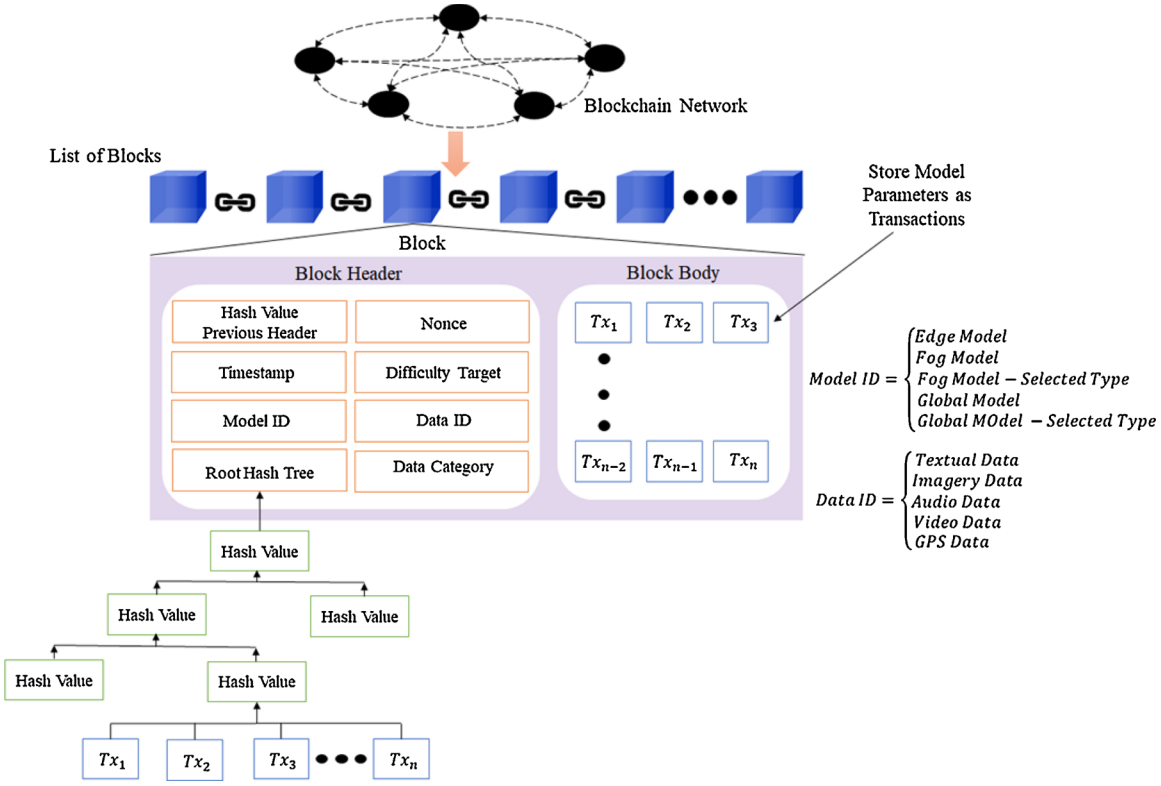


Fig. 2. Structure of the block in the blockchain network.

phase I, the edge nodes broadcast the proxy $EM_e(t)$ to the data layer to train the model based on the local train data available at data layer. To preserve the privacy-sensitive data, the device/organization/agency will only share the parameter based on the model train on local data. Validation is required at the edge node to make sure to prevent cyber-attacks such as malicious participant, data/model poisoning, avoid free ridding, etc. If the aggregated model is validated, it will be added in OffChain to make sure the quality of service during training phase. The

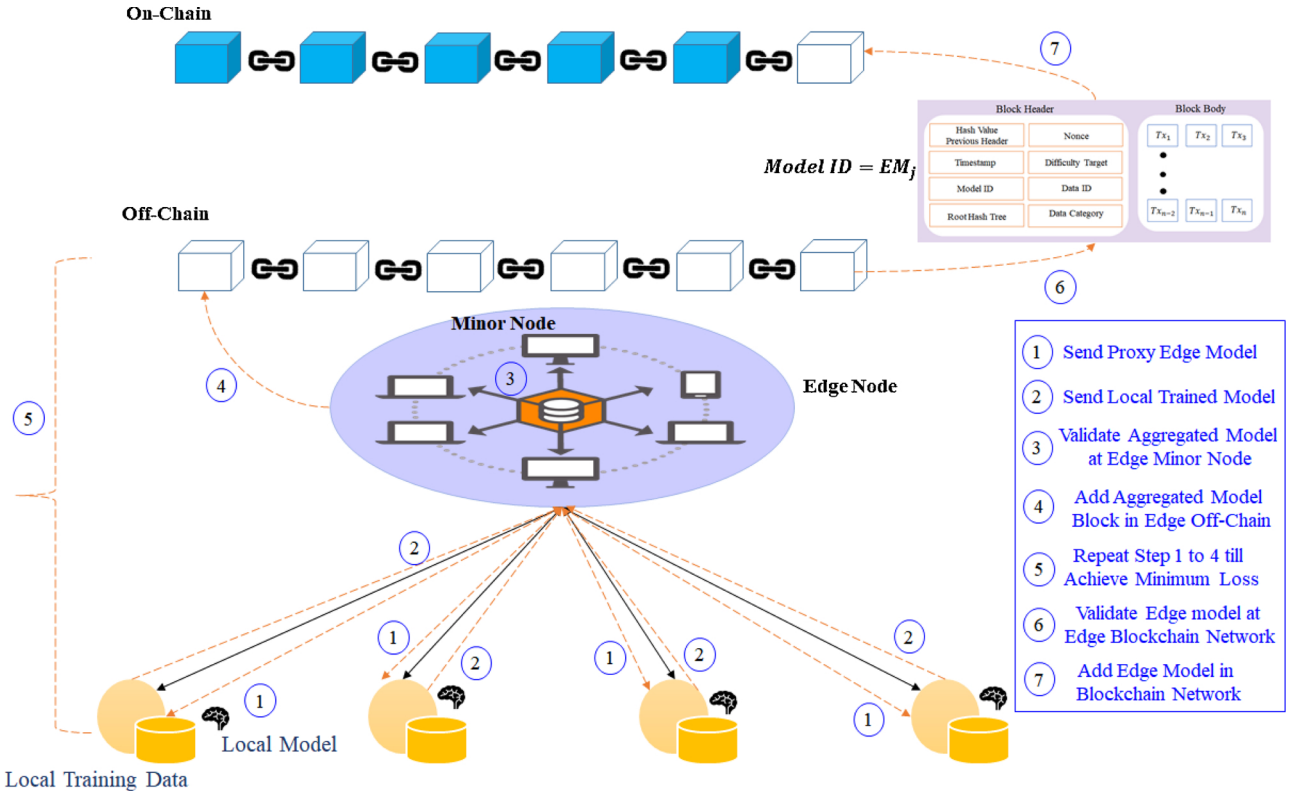


Fig. 3. Workflow of the proposed computing framework at the edge layer.

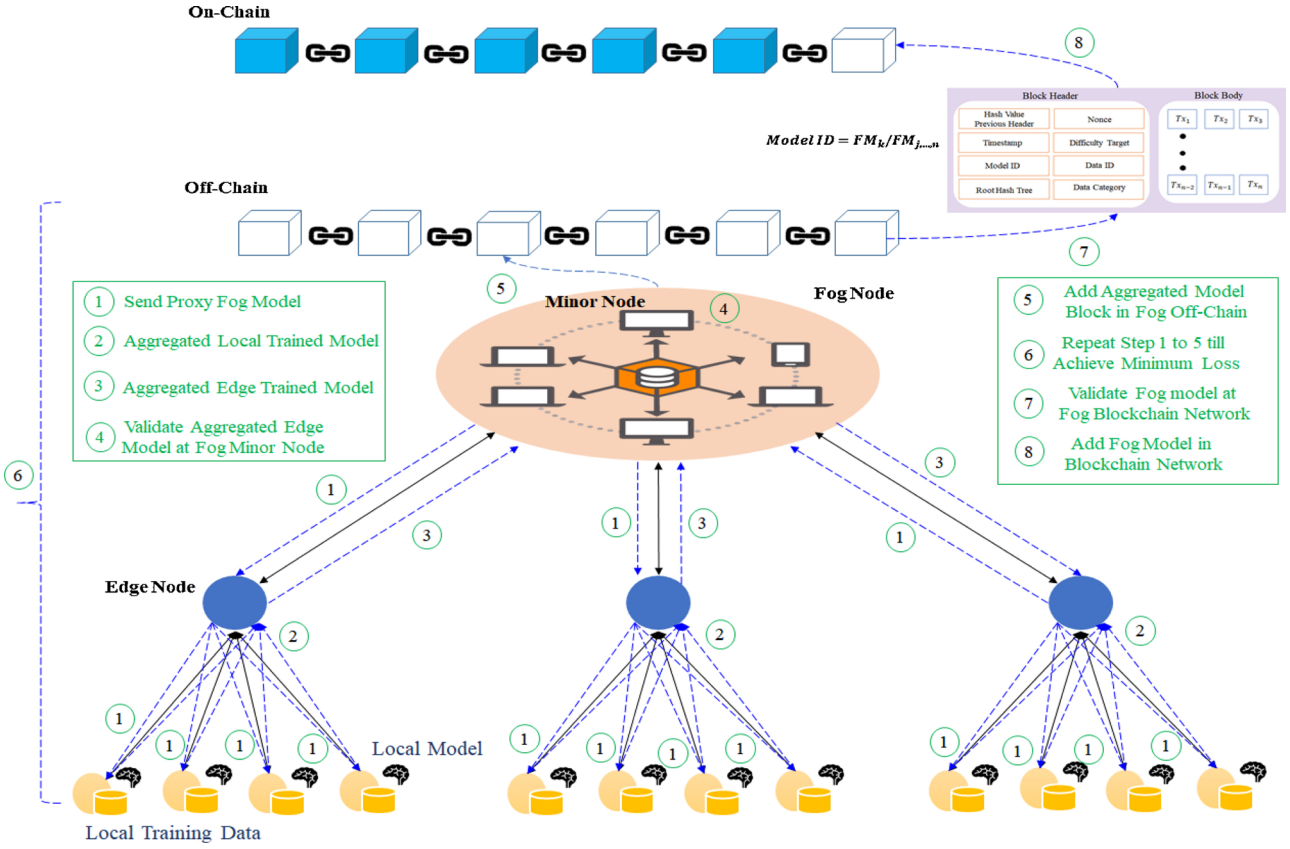


Fig. 4. Workflow of the proposed computing framework at the fog layer.

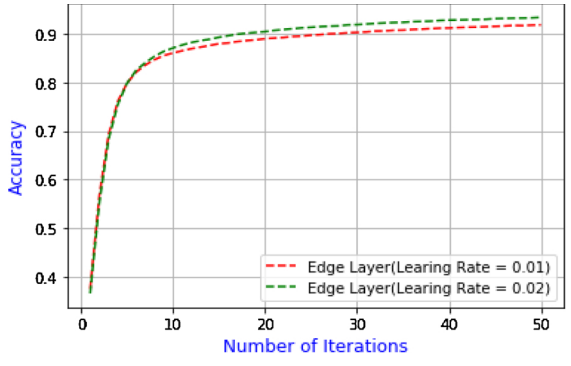
Table 1
Dataset consist of four different classes of image data.

Image Class	Features		Number of Samples
	Image Type	Size	
Airplane	Gray-level Image	32 × 32	6072
Bird			5000
Drone			500
Ship			5000

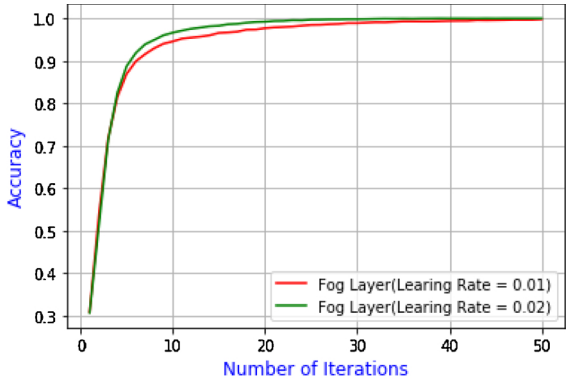
algorithm repeats the previous steps to reduce loss and achieve high accuracy. Finally, the algorithm will add the edge model in the Blockchain network. In phase II and III, the algorithm repeat the same process with additional features such as data type, data category to overcome the challenges of limited training data in order to obtain high accuracy and avoid reason specific model. We discuss the detailed structure of the block and the workflow of the proposed model in the next subsection.

3.3. Workflow of computing framework

Fig. 2 presents the structure of the block in the Blockchain network. In the block header, we have some additional tags such as Model ID, Data ID, and Data Category to represent the model more precisely. Here, Model ID represents the type of model parameters, the block is stored. Model ID can be an edge model, fog model, fog model-selected type, global model, and global model-selected type. The model with selected type is used to represent the train model based on selected local training data to obtain high accuracy and to avoid a region-

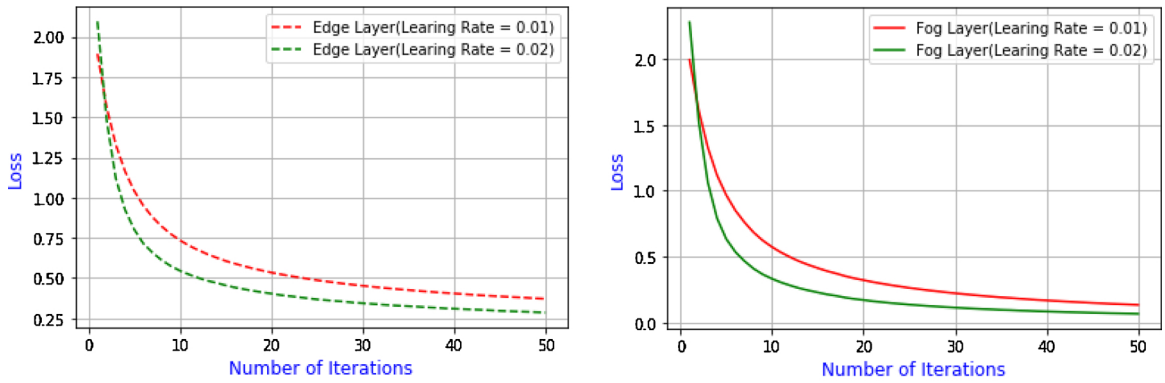


(a) Accuracy rate with fixed clients at edge layer



(b) Accuracy rate with fixed clients at fog layer

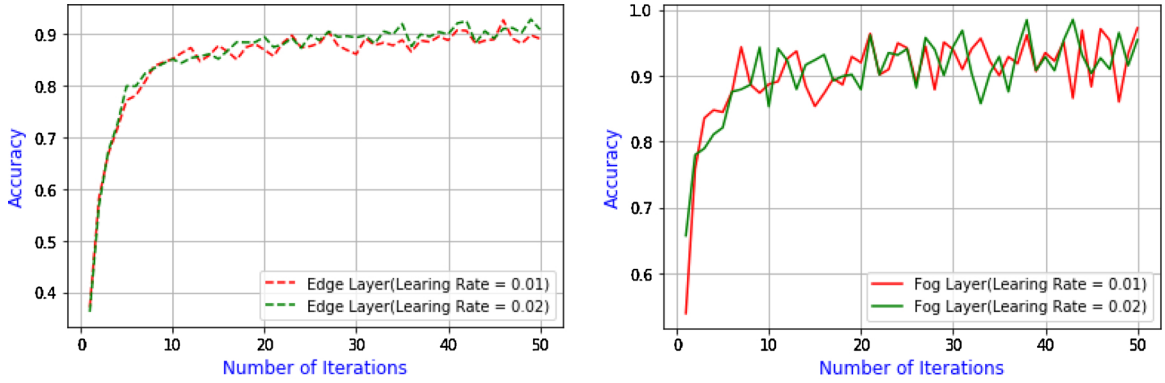
Fig. 5. Results of accuracy rate with fixed clients at both fog and edge layers.



(a) Loss rate with fixed clients at edge layer

(b) Loss rate with fixed clients at fog layer

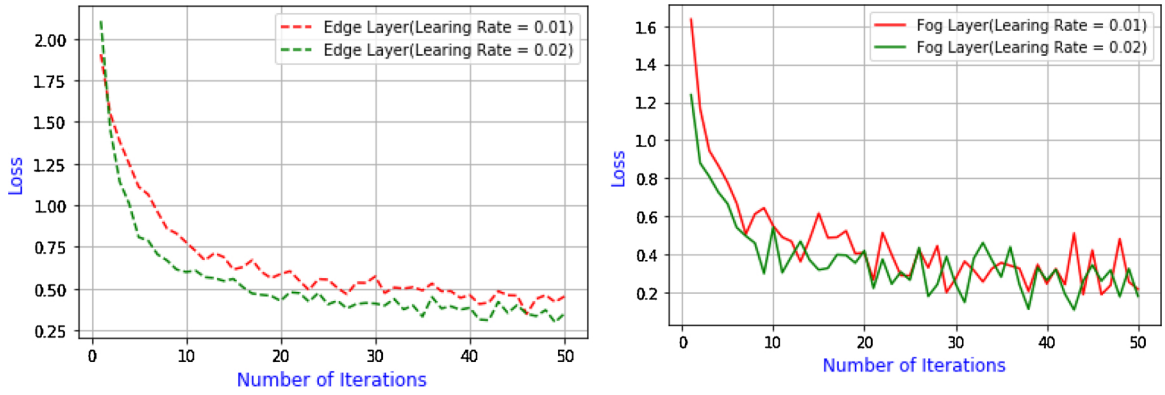
Fig. 6. Results of loss rate with fixed clients at both fog and edge layers.



(a) Accuracy rate with random clients at edge layer

(b) Accuracy rate with random clients at fog layer

Fig. 7. Results of accuracy rate with random clients at both fog and edge layers.



(a) Loss rate with random clients at edge layer

(b) Loss rate with random clients at fog layer

Fig. 8. Results of loss rate with random clients at both fog and edge layers.

specific model. In defence IoT, we could have the same category of dataset but located in different parts of the country. And due to privacy-sensitive data owing by the different organization/agency across the country, we are not allowed to share the data to any intermediary/servers. In such cases, in order to train the model with a large dataset to achieve high accuracy, the model with selected type will be a useful solution. With this solution, we can train our model with a large dataset to make the model decision more precise and accurate. Since we train the model at different layers, we assign different ID to each model to allow the user to choose the model to make the decision based on time, situation, complexity, and criticality. In the block header, we also have a Data ID tag to identify the type of training data. At data layer, the defence IoT can have different type of data collections such as textual, imagery, audio, video, and GPS data. In addition, the block header also have tag called Data Category to classify the category of data for which the model parameters are stored in the block body. For instance, in case of imagery data, the model can be trained based of different categories of data such as animals, birds, drones, human, battle weapons, etc. We describe the workflow of the proposed model at the edge and fog layers as follows.

Table 2
Presents the results of accuracy and loss at both fixed and random nodes (all scenarios).

Node Type	Layer	Learning Rate	No. of Iterations	Accuracy	Loss
Fixed Node	Edge	0.1	50	0.921	0.38
		0.2		0.946	0.27
	Fog	0.1		0.987	021
		0.2		0.969	0.13
Random Node	Edge	0.1		0.89	0.42
		0.2		0.92	0.36
	Fog	0.1		0.971	0.23
		0.2		0.965	0.19

3.3.1. Edge layer

Fig. 3 shows the workflow of the proposed computing framework at the edge layer. Each edge node consists of minor nodes that connect using the Blockchain technique to validate the transaction model. Each edge node maintains its own Offchain network to store the temporary blocks while training edge model using federated learning. All the edge nodes connected using the Blockchain technique to validate the new block in the Blockchain network. As shown in the Fig. 3, the edge node will initially broadcast the proxy edge model to all the nodes at data layer in step 1. In step 2, all the local nodes at the data layer will train the model using their own local training data. After aggregating the parameter of all the models received from the data layer, the aggregated model will validate by the minor nodes at the edge node. In step 4, the proposed framework will add the validated aggregated model to the Offchain network and continue the steps 1–4 of step 5 until the minimum loss or the threshold value is reached. In step 6, we will validate the generated edge model with the peer edge nodes to ensure that edge node is not compromised by a cyber-attack. Finally, the computing framework will add the new block in the Blockchain network with model ID EM_j. We use the Offchain network to provide the required services without compromising quality when training the edge model using recursive approach of federated learning.

3.3.2. Fog layer

The key advantage of the proposed computing framework with multi-layer computing nodes using federated learning is the global view of the local training data. To overcome the limitations of train the model with limited training data at each node of data layer, the proposed multi-layered modeling approach will be the robust solution in defence IoT. As shown in Fig. 4, the fog node initially broadcasts the proxy fog node model to all the lower layers nodes in step 1. Here, we can limit the local nodes at data layer to train the model in case of fog model-selected type. This feature facilitate the model to train with a large dataset. In steps 2 and 3, the parameters of the trained models will be aggregated to avoid discloser of local model update. Similar to edge layer, fog layer will also validate the aggregated trained model at fog node and add in its own Offchain network to steps 4 and 5. To achieve minimum loss and high accuracy, the proposed model repeats the steps 1–5 until the threshold reaches value in step 6. At last, the trained fog model/fog model-selected type will be validated among the peer fog nodes and will be added in the Blockchain network in steps 7 and 8. At cloud layer, we will follow the similar steps to train global model and global model-selected type.

4. Experimental analysis

4.1. Experimental setup

To evaluate the proposed model, we prepared the dataset for an experiment on classifying images using federated learning. This dataset consist of four different classes of image data i.e. “Airplane”, “Bird”, “Drone”, and “Ship” from the different sources (Bounding box detection of drones, 2019; CVonline, 2019). We preprocess each data into 32×32 Gy-level image. Table 1 summarizes the dataset features for different classes. There are 16,572 image data samples from which we randomly selected 80 % of the data for training and 20 % for testing the dataset. We randomly divided training dataset into 50 different clients and assigned each client with unique client ID. Each client ID represent its own local training dataset at data layer. We installed Tensorflow 2.0, Python 3.6, and Jupyter notebook to implement the proposed model prototype. In the implementation, we also installed tensorflow federated package for computation on decentralized data using federated learning. We investigate the performance of the proposed framework in various scenarios and discuss the results in next subsection.

4.2. Experimental results

In first scenario, we trained the proposed model using federated learning at the edge and fog layers with fixed clients. We observed the results of accuracy of the model trained at hyper leaning rate parameters 0.01 and 0.02, and 50 number of iterations. Fig. 5 shows the result of accuracy at both fog and edge layers. The result shows that the proposed model obtained an accuracy rate of 99.90 % (approx.) at the fog layer; while the accuracy rate at the edge layer is observed around 92 % (approx.) in 50 iterations. We also observed the rate of loss of the proposed model at the edge and fog layers. Fig. 6 shows the loss rate obtained at two layers with respect of number of iterations. The model outperforms the edge and fog layers at a learning rate of 0.02.

Since, in the case real-time applications, there will be a high probability that not all participants (i.e. clients with their own local training data) will be able to participate in all the iteration during the training phase. In this case, it is likely that the participant drop will occur during the training phase. To evaluate this scenario, in the second case, we also trained the proposed model using federated learning at the edge and fog layers with random clients at each iterations. Fig. 7 shows the rate of accuracy obtained at the edge and fog layers with a random selection of clients in each iterations. As we can see, there are fluctuations in the accuracy rate obtained due to random selections of local training data in each iteration. However, overall, the proposed model achieved an accuracy rate greater than 92.7 % (approx.) at the fog layer; while the accuracy of the rate at the edge layer is less than 90 %. Fig. 8 demonstrates the loss rate at the edge and fog layers with a random selection of clients in each iteration. Even though it was a random selection of local training data at each iteration, the proposed model achieved high accuracy and low loss in the fog layer. Table 2 represents the effectiveness and efficiency of the proposed model, and trains the model with high accuracy at multi-layered framework without sharing the local training data.

5. Conclusions

Currently, activities in combat zones are directed in a puzzled and problematic state for shorter periods of time in order to obtain an accurate assessment of the circumstances for making appropriate decisions. Defense-led combat using IoBT modifies the correspondence entries and associates the resources of the combat zone with the central command. In this research, we studied the limitation of defense system platform and proposed a distributed computing framework. The proposed multi-layered model effectively utilize the features of blockchain technology and federated learning to provide a distributed platform for defence IoT. We prepared the dataset for classification of image in the combat zone using the proposed model. The results of the simulation showed that the proposed model is adequate enough to train the model to make decision with high accuracy without sharing the local training data. The proposed model has limits in terms of incentive scheme for participants in the local node during the training process. In the future, we will add the features of the incentives to the local training node for participation in the training process and reward it the according to the

percentage of contribution.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

This research was supported by BK21 Plus project of the National Research Foundation of Korea Grant and was supported by the Dongguk University Research Fund of 2020.

References

Abdelzaher, T., Ayanian, N., Basar, T., Diggavi, S., Diesner, J., Ganesan, D., ... Nahrstedt, K. (2018a). Toward an internet of battlefield things: A resilience perspective. *Computer, 51*(11), 24–36.

Abdelzaher, T., Ayanian, N., Basar, T., Diggavi, S., Diesner, J., Ganesan, D., ... Nahrstedt, K. (2018b). Will distributed computing revolutionize peace? The emergence of battlefield iot (2018, July) *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)* (pp. 1129–1138).

Ande, R., Adebisi, B., Hammoudeh, M., & Saleem, J. (2019). Internet of Things: Evolution and technologies from a security perspective. *Sustainable Cities and Society,* 101728.

Bounding box detection of drones (small scale quadcopters) with CNTK Fast R-CNN, https://github.com/creiser/drone-detection, accessed 23 Dec 2019.

CVonline: Image Databases, http://homepages.inf.ed.ac.uk/rbf/CVonline/Imagedbase.htm, accessed 23 Dec 2019.

Defense Policy and the Internet of Things Disrupting Global Cyber Defenses, https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-IoT-defense-policy-and-the-internet-of-things.pdf, accessed 23 Dec 2019.

Farooq, M. J., & Zhu, Q. (2017). Secure and reconfigurable network design for critical information dissemination in the internet of battlefield things (IoBT) (2017, May) *2017 15th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)* (pp. 1–8).

He, S., Zeng, W., Xie, K., Yang, H., Lai, M., & Su, X. (2017). PPNC: Privacy preserving scheme for random linear network coding in smart grid. *Transactions on Internet and Information Systems, 11*(3).

IoT In Aerospace & Defense Market, https://www.alliedmarketresearch.com/internet-of-things-in-aerospace-and-defense-market, accessed 23 Dec 2019.

Jalaian, B. A., Koppel, A., Harrison, A., Michaelis, J., & Russell, S. (2018). On stream-centric learning for internet of battlefield things (2018, March) *In 2018 AAAI Spring Symposium Series*.

Khan, F. A., Asif, M., Ahmad, A., Alharbi, M., & Aljuaid, H. (2020). Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. *Sustainable Cities and Society,* 102018.

Kim, H., Park, J., Bennis, M., & Kim, S. L. (2019). Blockchained on-device federated learning. *IEEE Communications Letters*. https://doi.org/10.1109/LCOMM.2019.2921755,2019.

Konečný, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., & Bacon, D. (2016). *Federated learning: Strategies for improving communication efficiency*. arXiv preprint arXiv:1610.05492.

Kott, A. (2018). Challenges and characteristics of intelligent autonomy for internet of battle things in highly adversarial environments (2018, March) *018 AAAI Spring Symposium Series*.

Kott, A., Swami, A., & West, B. J. (2016). The internet of battle things. *Computer, 49*(12), 70–75.

Laufs, J., Borrion, H., & Bradford, B. (2020). Security and the smart city: A systematic review. *Sustainable Cities and Society,* 102023.

Lee, W., Kim, N., & Lee, B. D. (2019). An adaptive transmission power control algorithm for wearable healthcare systems based on variations in the body conditions. *Journal of Information Processing Systems, 15*(3).

Lever, K. E., & Kifayat, K. (2020). Identifying and mitigating security risks for secure and robust NGI networks. *Sustainable Cities and Society,* 102098.

Lin, K., Xia, F., Li, C., Wang, D., & Humar, I. (2019). Emotion-aware system design for the battlefield environment. *Information Fusion, 47*, 102–110.

Lu, Y., Huang, X., Dai, Y., Maharjan, S., & Zhang, Y. (2019). Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Transactions on Industrial Informatics*. https://doi.org/10.1109/TII.2019.2942190,2019.

Mohammadi, V., Rahmani, A. M., Darwesh, A. M., & Sahafi, A. (2019). Trust-based recommendation systems in Internet of Things: A systematic literature review. *Human-centric Computing and Information Sciences, 9*(1), 21.

Nieto, A., & Rios, R. (2019). Cybersecurity profiles based on human-centric IoT devices. *Human-centric Computing and Information Sciences, 9*(1), 39.

Rathore, S., Kwon, B. W., & Park, J. H. (2019). BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. *Journal of Network and Computer Applications, 143*, 167–177.

Ren, Y., Leng, Y., Zhu, F., Wang, J., & Kim, H. J. (2019). Data storage mechanism based on blockchain with privacy protection in wireless body area network. *Sensors, 19*(10), 2395.

Ren, Y., Zhu, F., Sharma, P. K., Wang, T., Wang, J., Alfarraj, O., & Tolba, A. (2020). Data query mechanism based on hash computing power of blockchain in internet of things. *Sensors, 20*(1), 207.

Ren, Y., Liu, Y., Ji, S., Sangaiah, A. K., & Wang, J. (2018). Incentive mechanism of data storage based on blockchain for wireless sensor networks. *Mobile Information Systems, 2018*.

Russell, S., & Abdelzaher, T. (2018). The internet of battlefield things: The next generation of command, control, communications and intelligence (C3I) decision-making (2018, October) *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)* (pp. 737–742).

Sharma, P. K., Kumar, N., & Park, J. H. (2020). *Blockchain technology toward green IoT: Opportunities and challenges.* IEEE Networkhttps://doi.org/10.1109/MNET.001.1900526.

Singh, S. K., Rathore, S., & Park, J. H. (2019). Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. *Future Generation Computer Systems*.

Sirko, S., Kozuba, J., & Piotrowska-Trybull, M. (2019). The military's links with local communities in the context of sustainable development. *Sustainability, 11*(16), 4427.

Smaliukiene, R. (2018). Sustainability Issues in the military: GENESIS AND PROSPECTS. *Journal of Security and Sustainability Issues, 8*(1).

Suri, N., Tortonesi, M., Michaelis, J., Budulas, P., Benincasa, G., Russell, S., ... Winkler, R. (2016). Analyzing the applicability of internet of things to the battlefield environment (2016, May) *2016 International Conference on Military Communications and Information Systems (ICMCIS)* (pp. 1–8).

The Internet of Things for Defense, http://www.windriver.com/whitepapers/iot-for-defense/wind-river_%20IoT-in-Defense_white-paper.pdf, accessed 23 Dec 2019.

Tosh, D. K., Shetty, S., Foytik, P., Njilla, L., & Kamhoua, C. A. (2018). Blockchain-empowered secure internet-of-battlefield things (iobt) architecture (2018, October) *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)* (pp. 593–598).

Wang, J., Yang, Y., Wang, T., Sherratt, R. S., & Zhang, J. (2020). Big data service architecture: A survey. *Journal of Internet Technology, 21*(2), 393–405.

Xia, Z., Fang, Z., Zou, F., Wang, J., & Sangaiah, A. K. (2019). Research on defensive strategy of real-time price attack based on multiperson zero-determinant. *Security and Communication Networks, 2019*.

Xia, Z., Tan, J., Wang, J., Zhu, R., Xiao, H., & Sangaiah, A. K. (2019). Research on fair trading mechanism of surplus power based on blockchain. *Journal of Universal Computer Science : J UCS, 25*(10), 1240–1260.

Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology (TIST), 10*(2), 1–19.