Fog Intelligence for Secure Smart Villages: Architecture, and Future Challenges

Aljuhani Ahamed, Kumar Prabhat, Kumar Randhir, Jolfaei Alireza, Islam A.K.M. Najmul

DOI: 10.1109/MCE.2022.3193268

Fog Intelligence for Secure Smart Villages: Architecture, and Future Challenges

Ahamed Aljuhani
University of Tabuk, Saudi Arabia.

Prabhat Kumar
LUT University, Lappeenranta, Finland.

Randhir Kumar
Indian Institute of Technology Hyderabad, India.

Alireza Jolfaei
Flinders University, Adelaide, Australia.

A. K. M. Najmul Islam
LUT University, Lappeenranta, Finland.

***Abstract*—The Internet of Things (IoT) technology is seen as the foundation for next-generation smart villages due to its ability to use sustainable information and communication technologies. The smart villages can enable real-time data analytic and can automate decision making for local villagers in terms of agriculture, healthcare, transportation, environment, and energy. However, most of the wireless sensing devices exchange information using public network and therefore may not be able to resist all forms of attacks. Additionally, most of the IoT devices are resource restricted and uses cloud servers to process and store data. However, when IoT devices communicate with cloud computing data centers, the volume of data causes network congestion. To provide secure services close to end devices, a new network architecture called Distributed Fog Computing (DFC) can be created and integrated with IoT-based smart villages deployment. Motivated from the aforementioned discussions, this article explores the integration of DFC with IoT in improving security and privacy solutions for villagers and Consumer Electronic (CE) devices. As a case study, we also design and evaluate the performance of an Intrusion Detection System (IDS) in DFC-based smart village environment. Finally, we discuss several open security issues and challenges regarding Fog-to-Things enabled smart villages.**

INTRODUCTION The rapid evolution of technologies and communications raises the demand for emerging smart paradigms, such as the Internet of Things (IoT). The IoT aims to transform "things" from conventional to a smart object, enabling multiple connected devices to send, process, and receive data across multiple locations with minimal or no human involvement. Such a technology provides several great features to end users, including cost reduction, automation, real-time analysis, improving productivity, and better business opportunities. As IoT plays a significant role in turning "things" to be smart based on technology, a diverse range of critical sectors, such as energy, transportation systems, industrial, communication, and healthcare, have employed IoT technology as an integral part of smart system operations. The number of IoT connected devices has been growing exponentially

Published by the IEEE Consumer Technology Society

and might reach 27 billion connected devices by 2025 [1]. Thus, from consumer perspectives, IoT should be centered on providing safe and automated infrastructure in living and non-living environment.

Recently, the IoT technology plays a vital role in smart villages to provide cost-effective and efficient solutions for villagers. As the majority of people in different countries live in rural settlements with minimum technology and resources, this offers several opportunities for developing IoT applications in different important domains within rural settlements [2]. For example, villagers regularly use traditional crop harvesting methods, making farm management extremely difficult. A smart village includes Agricultural Internet of Things, which can help farmers deal with all of the issues associated with farming, such as weather and water management. The use of IoT applications and services in such a village will improve quality of life by providing a resilient, cost-effective, and sustainable smart village [3]. Even though IoT-based smart villages improve the quality of villagers' lives, it is still critical to develop rural areas as smart villages with lack of technology resources, such as computational and communication infrastructure. To address these issues, fog computing is a new emerging technology that enables storage, communication, and network functions in a distributed fashion [4]. The main principle of fog computing is to extend the cloud closer to IoT devices, acting as an intermediate layer between the IoT end user and the cloud.

Cloud technology has several limitations, such as latency, volume, limited bandwidth, data protection, and internet connectivity. To provide secure, robust, and safe telecommunication infrastructures, fog computing offers a great opportunity to improve the quality of life for villagers and IoT-enabled smart village Consumer Electronics (CE) devices by offloading security features to multiple fog nodes, and providing real-time cyberattack detection near to the data source (See Fig. 1). However, fog computing is not a replacement for cloud computing but it functions as an extension of the cloud. Fog computing is considered to be an implementation or evolution of Edge computing, which is another network paradigm that enables technologies to allow computation performed at the edge of the network, closer to the data generation points, i.e., sensors [5]. Fog computing shifts the data process into a fog node or IoT gateway, which is located within the Local Area Network (LAN). This is physically more distant from sensors. In addition, the flexibility of placing fog nodes anywhere between devices and the cloud is the most significant feature that distinguishes fog computing from several implementations of edge computing [5].

Figure 1: Fog computing improved security and privacy services in IoT-based smart villages.

Although IoT-based smart villages aim to facilitate human life and ameliorate the Quality of Service (QoS) in several domains, its security issues remain a big challenge [6]. As the combination term of "smart" and "things" often refers to a technology like IoT, the deployment of such a technology in villages introduces several cyber threats worth investigating. A sybil attack, for example, is one type of security threat in which an attacker may exploit vulnerabilities in smart village networks. In a sybil attack, a malicious node falsifies its identity and broadcasts excessively incorrect information to legitimate nodes, causing a node's resources to be completely drained [7]. In addition, scanning attack could pose a major risk as such an attack scans vulnerabilities in smart village devices and perform malicious activities. Another well-known cyber threat is the man-in-the-middle attack, in which an adversary intercepting the network communication between connected smart village devices acts as a legitimate device to eavesdrop and steal sensitive information.

Following this introduction, this article discusses the integration of Distributed Fog Computing (DFC) with IoT-based smart villages to improve security and privacy services. In addition, this article discusses Security-by-Design (SbD) for an Intrusion Detection System (IDS) based on DFC in IoT-enabled smart villages, and explores the potential uses of other emerging technologies with such an environment. We also design and implement an IDS for DFC-based smart village as a case study. Finally, this article discusses several open security issues and recommendations regarding Fog-to-Things enabled smart villages.

1. Distributed fog computing-enabled IDS

The integration of fog computing and IoT has driven Fog-of-Things (FoT) to overcome the cloud limitations and provide several advantages. Fog computing improves the security and privacy of IoT-enabled smart villages from many perspectives. One of the distinctive features of fog computing is that it provides a distributed computing environment, unlike cloud computing, which follows a centralized architecture [6]. Therefore, DFC can be utilized to provide distributed security solutions such as IDS. Due to a large amount of heterogeneous data generated from IoT devices, requiring rapid, efficient, and real-time response, DFC improves the computational resource of IDS as a security function closer to the network edge, which helps provide a lightweight, efficient, and rapid mitigation response against several cyber security threats. As fog computing enables deploying parallel and distributed security solutions, IDS can be implemented as distributed security functions at multiple fog nodes in the context of Fog-to-Things architecture, which enables a collaborative detection and mitigation approach that can share and exchange data to provide an effective and robust mitigation approach against several cyber attacks. Moreover, IDS can benefit from DFC in providing low latency that allows rapid response, resulting in decreasing potential damages caused by such attacks.

Several approaches can be implemented to achieve a collaborative IDS in fog computing; however, Fog-to-Things IDS architecture has several advantages, as it fully leverages the benefits of distributed fog nodes in terms of data processing, storage, latency, and scalability. In addition, the recourse constraints of IoT devices that require lightweight detection are closer to applications and in the proximity of IoT nodes. Therefore, utilizing fog architecture in detecting several cyber threats, such as man-in-the-middle, sniffing, and eavesdropping attacks, is more effective compared with the cloud [8]. As Fig. 2 shows, the detection model is hosted locally at each node, while the master fog node performs the computation and updates the detection model parameters to each node. The architecture reveals that the data can be trained and validated at a single node, and distributes the model parameters in parallel to each node, enabling a collaborative intrusion detection closer to IoT devices while distributed detection nodes exchange the learning parameters with its neighbor nodes through the master fog node. The Fog-to-Things IDS architecture allows the building of a lightweight, scalable, and rapid detection approach that can effectively and efficiently mitigate several cyber threats.

2. IDS-based emerging technology in fog computing

The IDS as a security service can be improved with emerging technologies as well as benefit from the architecture of DFC paradigm in order to enable a secure IoT-based smart village that can be effectively and efficiently combat several cyber threats. We discuss SbD for the possible integration of emerging technologies with IDS-based DFC to improve security and privacy solution in smart villages.

2.1. 5G Networks

The new generation of wireless network technology promises a significant revolution in wireless connectivity and network communications. As the IoT environment contains a large number of connected devices from several smart domains, which communicate with different network topology and protocols, the 5G networks provide several benefits over current cellular networks including fast data transmission, low latency, improved capacity, and enhanced coverage for Machine Type Communication (MTC). The 5G networks also can be a complement with fog computing as such an environment cooperate with different network layers requiring fast, reliable, and efficient machine to machine communication. As the nature of fog computing reveals a decentralized architecture that requires high frequency transmission rate with minimum delay among distributed Fog nodes, such a collaborative security function like a distributed IDS can leverage the benefits of 5G technology with fog computing in providing rapid and effective security attack mitigation.

2.2. Artificial Intelligence

Artificial Intelligence (AI) plays a vital role in smart technology and has potential uses of its applications within critical domains in smart villages. When speaking of AI, machine learning and deep learning (ML/DL) have gained much attention in detecting malicious activities and reducing damages to the systems when integrated with security functions such as IDS. The IDS can be employed as a collaborative detection model based on ML/DL techniques, leveraging the

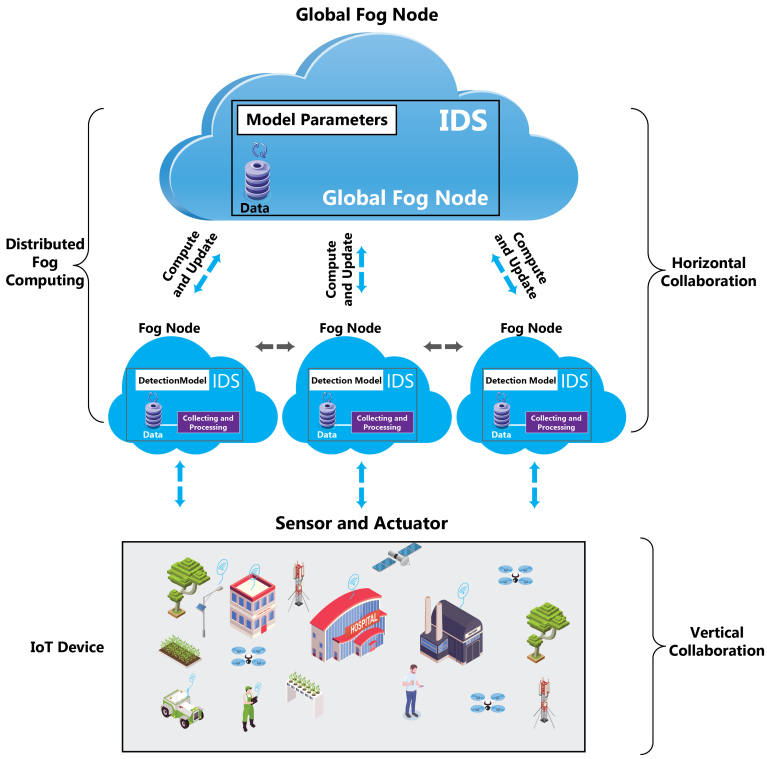

Figure 2: The Fog-to-Things distributed IDS architecture in IoT-based smart villages.

computational resources and low latency that are provided by DFC to analyze, classify, and mitigate attacks effectively on real-time [9]. Such features of DFC help develop a lightweight, efficient, and rapid mitigation mechanism based on ML/DL techniques, reducing the risk caused by cyber threats in smart villages.

2.3. Software Defined Network

Fog computing can employ software-defined networking (SDN) and benefit from its significant features. SDN is a network architecture paradigm that enables a network topology to be managed and programmed by software applications. As the SDN controller is considered the most important function of SDN architecture, the fog layer can utilize the SDN controller to provide the anomaly detection approach where the network traffic has to go through a fog node or a fog server, in which the SDN controller is hosted [10]. The detection and mitigation mechanism provides the controller with updated flow rules to segregate and disregard malicious traffic from legitimate traffic. Fog computing provides sufficient computational resources for such an implemented detection algorithm based on an SDN controller.

2.4. Network Functions Virtualization

In addition to the SDN, network functions virtualization (NFV) is an emerging technology that employs virtualization concepts to its network functions, decoupling network components from underline hardware to be all virtualized network functions running as software on standard servers. As fog computing operates in a virtualized intermediate layer and virtual machines can be dynamically instantiated and removed, the NFV paradigm will benefit fog computing by virtualizing different network functions, such as switches, IDS, load balancers, and firewalls, and operating those instances over fog nodes [11]. NFV also provides flexibility to its virtualized security functions (VSFs), such as intrusion detection and prevention systems, by adapting new rules or instantiating new security instances on demand.

2.5. Blockchain

Blockchain technology has been employed with several emerging technologies, such as the IoT ecosystem. Blockchain technology follows the decentralized architecture by its nature, which can help provide decentralized security services for an IoT-based smart

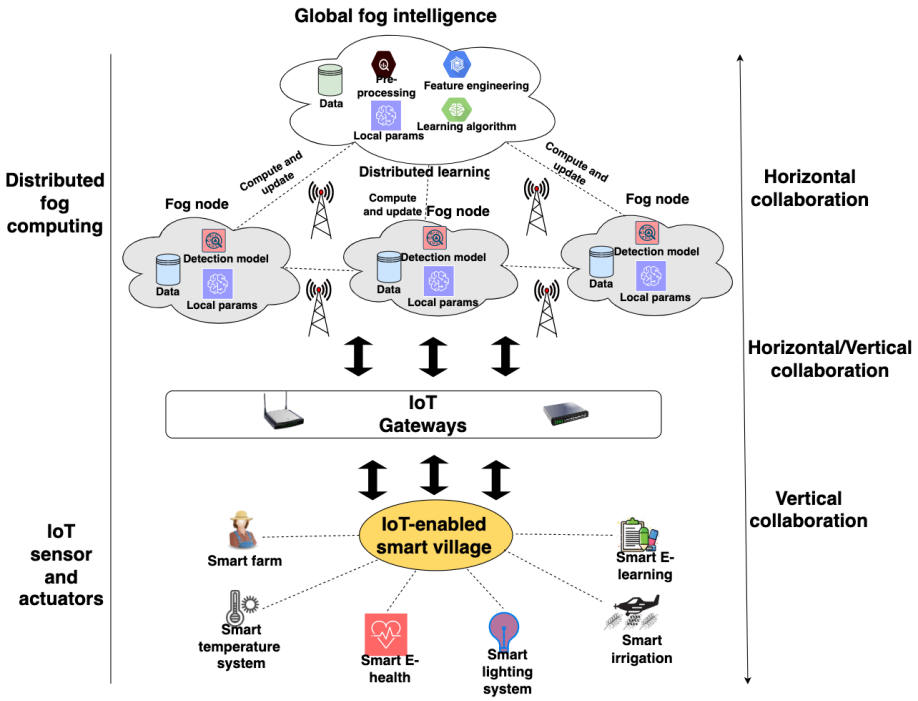

Figure 3: Case study of distributed fog computing for secure smart village.

village ecosystem. A distributed IDS gains several advantages over a single IDS in detecting sophisticated attacks. Moreover, distributed IDS nodes need to collaborate and exchange data efficiently and effectively between IDS nodes to detect and mitigate a diverse range of cyber threats. However, two major challenges with distributed IDS have been observed [12], [13]: sharing the information among multiple IDS nodes and computation trust between participants. To resolve these issues, blockchain technology ensures the integrity of data when sharing and exchanging information among multiple IDS nodes through building a trust management model for data sharing. With the advent of fog computing, fog nodes can communicate with each other by using blockchain technology without involvement of a centralized authority or third party in the Cloud, which helps avoid the single point of failure problem [12]. Blockchain technology has strong potential and can be integrated with other emerging technology, such as SDN and fog computing, to provide a secure, resilient, and more efficient mitigation system against several cyber threats in IoT-based smart villages.

2.6. Big data analytic

The massive amount of heterogeneous data produced from IoT devices requires a cost-effective and efficient computational resources method to process, analyze, and filter big data near IoT devices. The architecture of DFC provides fog data services, which comprise several functionalities such as data management, data analysis, data security, and data virtualization [14]. With such features of data services in fog architecture, the distributed fog nodes help analyze data in real time, providing rapid and efficient decision making near the IoT sensors. Such a lightweight analytical tool implemented based on machine learning techniques (TinyML) will help in analyzing data and selecting the most important features in classifying and detecting attacks effectively.

3. Case study of distributed fog computing for secure smart village

As a case study, we have designed and implemented an IDS based on XGBoost and Random Forest using DFC. Fig. 3 shows general architecture of our proposed distributed and parallelized attack detection process in IoT-based smart village scenario. In this case study, we have several IoT sensors and actuators responsible for capturing real-time data from their surroundings and transmitting to near by fog nodes for further processing. Once the data is received by the nearest worker fog nodes, they compute the gradient and sends the partial gradient to master fog node.

Table 1: Per-class prediction results (%) for proposed IDS on ToN-IoT dataset.

Model	Parameters	Backdoor	DDoS	DoS	Injection	MITM	Normal	Password	Ransomware	Scanning	XSS
XGBoost	PR	99.41	98.14	97.96	97.16	98.72	99.99	99.85	98.85	99.11	98.53
	DR	99.10	97.17	98.98	98.03	86.94	100.00	99.39	99.98	97.38	99.88
	F1	99.85	97.14	98.47	97.59	92.54	99.99	99.89	99.88	99.11	99.59
	FAR	0.00002	0.00120	0.00091	0.00120	0.00002	0.00011	0.00008	0.00051	0.00001	0.00002
Random Forest	PR	99.97	97.14	96.96	98.16	97.91	99.77	99.19	98.87	99.96	98.52
	DR	99.82	97.12	98.98	98.03	89.11	100.00	99.37	99.21	97.38	99.93
	F1	99.66	97.16	98.27	97.60	92.24	99.77	99.59	99.34	99.16	98.67
	FAR	0.00002	0.00118	0.00097	0.00136	0.00002	0.00012	0.00009	0.00122	0.00002	0.00003

Terms & Abbreviations: PR:Precision Rate; DR: Detection Rate; FAR: False Alarm Rate.

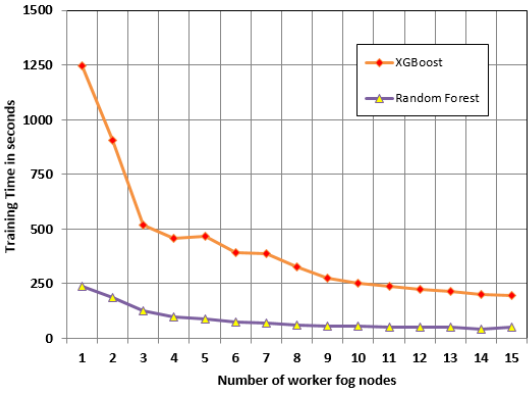

Figure 4: Training time analysis by varying fog nodes

The master fog node aggregates the gradients from all worker fog nodes and send backs the new weight to worker fog nodes. The gradients are further used and we get attack detection models as an output from the worker fog nodes. This sharing reduces overall training time in real-time and increases the efficiency of attack detection process. The proposed IDS is based on three different steps.

- Data acquisition and pre-processing: In particular, actual IoT datasets obtained from IoT environment is used to simulate the proposed IDS. The initial features are pre-processed to make datasets more generalized and compatible for learning algorithms.
- Distributed Learning in fog environment: The learning algorithms are implemented and trained on multiple fog nodes. This process can be executed on routing and switching devices of smart village.
- Attack detection: This phase use the knowledge obtained from training to detect attacks.

3.1. Performance Evaluation

The above steps are used to design and simulate the proposed IDS. The overall experiments of this study were performed on an Intel(R) Xeon(R) Silver 4114 CPU @ 2.20 GHz (2 processors), 128 GB RAM, and a 2 TB hard disk. We have used Kubernetes and H2O.ai platform to train and test the proposed IDS. The parallelism and distribution is carried out by varying number of machines used during training. The ToN-IoT dataset is used to show the effectiveness of the proposed model [8]. This dataset contains various recent attacks such as, backdoor, DoS, DDoS, injection, MITM, password, ransomware, scanning and XSS attacks, that are mostly found in IoT-based smart village environment. The algorithms mentioned in [13] were used to design proposed IDS using DFC. Fig. 4 shows the training time for XGBoost and Random Forest using 15 fog nodes. It is seen that the training time decreases with increase in worker fog nodes. We have used multiple evaluation metrics such as Detection Rate (DR), Precision (PR), F1 and False Alarm Rate (FAR) to evaluate the performance of the proposed IDS as mentioned in [13]. Table 1 shows per-class prediction results using ToN-IoT dataset. It is worth noting that the performance of both algorithms on ToN-IoT dataset is effective and has obtained higher values i.e., 86-100% for different evaluation metrics. Moreover, we see that the FAR for the attack groups have been reduced close to 0%. This indicates that the DFC-enabled IDS has huge potential in detecting attacks in real-time IoT-based smart villages environment. Finally, we have compared our work with some recent state-of-the-art techniques using ToN-IoT dataset. Table 2 shows the comparison in terms of overall accuracy. It is seen that the proposed distributed IDS has achieved 99.89% and 98.31% accuracy with XGBoost and random forest, respectively. This is higher compared to the works presented in [15] and [8].

4. Security issues and challenges

Although the integration of fog computing in a smart village provides considerable advantages to end users, security and privacy issues remain significant challenges. We briefly discuss the major security and privacy challenges in the integration of fog computing with IoT-based smart villages.

Table 2: Performance comparison with existing state-of-the-art techniques

Authors	Mechanism	Method	Accuracy
Alsaedi et al. [15]	Centralized	CART	77.00%
		LSTM	68.00%
Lo et al. [8]	Centralized	E-GraphSAGE	97.87%
Proposed IDS	Distributed	XGBoost	99.89%
		Random Forest	98.31%

Terms & Abbreviations: CART: Classification and Regression Trees; LSTM: Long Short-Term Memory

4.1. Authentication

The nature of IoT technology requires devices to prove their identity and ensure that IoT devices can be trusted to connect and exchange data among IoT objects and fog nodes. Authentication of devices is important to avoid cyber attacks, such as man-in-the-middle attacks. Many proposed authentication schemes were presented in the previous work; however, traditional authentication approaches are insufficient and lack scalability. Therefore, a lightweight authentication protocol is needed to meet the security requirements between IoT devices and fog nodes [15]. As fog computing authenticates many end users' devices simultaneously, to become a part of the network, it lacks real-time interaction and causes high latency. Another challenge of authentication is regarding trust and service level agreement (SLA) between different members of interconnected services, while designing a mutual authentication scheme is another obstacle.

4.2. Access control

Access control is one of the major security protection approaches that entails protecting, preserving, and restricting access to a user's data or a service from unauthorized access, and allowing the credentials for only authorized entities. The main objective of access control is to maintain security and privacy for end users and protect data from attacks that attempt to gain unauthorized access and perform malicious activities. Due to the involvement of different members of interconnected services, "IoT-Fog-Cloud," maintaining access control between a large group of different service providers becomes a challenge. As fog computing comprises many fog nodes and data is transmitted among those nodes, it may trigger time delay and result in a high latency issue, which affects the access decision to be within an acceptable time [15]. Preserving the privacy state while transmitting data from one domain to another through fog access control is another challenge in terms of maintaining the user's security and privacy requirements.

4.3. Data Privacy

With the rapid growth of several emerging technologies that deal with users' data, privacy constantly becomes a major concern. When discussing privacy, the main issues center on how the data is collected, shared, and stored. Due to the increasing number of interconnected devices and emerging new technologies that may be integrated with other technology architectures, users' privacy becomes a crucial part to maintain and control. An example is sharing users' data across multiple domain architectures, such as IoT-Fog-Cloud. As fog computing follows a distributed architecture, in other words, multiple fog nodes scattered and distributed over large areas, maintaining data privacy across multiple nodes in different locations becomes another challenge [15]. Moreover, fog nodes receive and process data at different fog storage levels and forward user's data to the cloud, such an attack on fog node storage will reveal sensitive user's data. Therefore, designing new solutions for ensuring data privacy is another major challenge.

4.4. Trust management

Trust management is an essential part to be maintained and established to identify a trusted node and isolate a malicious node before it is connected to the network. Due to the nature of the fog environment, which includes scattered and distributed fog nodes over large areas, defining and maintaining the trust status of each node to determine whether a node is trustworthy or not becomes a challenge. Another trust management challenge is the integration of multiple environments, such as Things-Fog-Cloud, which reveals a centralized architecture for the cloud and a distributed environment for fog computing. Consequently, designing and maintaining trust management among distributed fog nodes is a research issue [13].

4.5. Virtualization Technologies

The primary purpose of network function virtualization (such as software defined networking (SDN) and network function virtualization (NFV)) is to enhance network performance while enhancing the network infrastructure's programmability and flexibility. In IoT-based smart villages, the inherent constraints in adapting such virtualized infrastructure are ensuring low latency, high throughput and minimal computation overheads.

4.6. Transition from 5G to Beyond 5G

The introduction of 5G and the shift to beyond 5G may present possible issues for carrier access networks in large-scale DFC installations of IoT-based smart villages (for example interconnections and interfaces, coordination,, administration and control, and interconnections between mobile, user plane function and fixed carriers).

5. Conclusion

In this article, we have explored the integration of distributed fog computing with IoT-based smart villages to improve the quality of life for villagers and consumer electronic devices from a security and privacy perspective. We have discussed Security-by-Design for intrusion detection system with the integration architecture of distributed fog computing in IoT-based smart villages. This article also presented possible integration of several emerging technologies with the IDS-based distributed fog computing to improve security and privacy solutions in a smart village. We also design and implement an intrusion detection system for distributed fog computing-based smart village as a case study. In the end, we discussed various security and privacy challenges that require attention from the research community.

REFERENCES

1. M. Hasan, "State of iot 2022: Number of connected iot devices growing 18% to 14.4 billion globally," 2022, online; accessed 25-May-20222. [Online]. Available: https://iot-analytics.com/number-connected-iot-devices/
2. P. K. Malik, R. Singh, A. Gehlot, S. V. Akram, and P. K. Das, "Village 4.0: Digitalization of village with smart internet of things technologies," *Computers & Industrial Engineering*, vol. 165, p. 107938, 2022.
3. P. Chanak and I. Banerjee, "Internet of things-enabled smart villages: Recent advances and challenges," *IEEE Consumer Electronics Magazine*, 2020.
4. K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "A systematic survey of industrial internet of things security: Requirements and fog computing opportunities," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2489–2520, 2020.
5. M. De Donno, K. Tange, and N. Dragoni, "Foundations and evolution of modern computing paradigms: Cloud, iot, edge, and fog," *Ieee Access*, vol. 7, pp. 150 936–150 948, 2019.
6. J. Singh, P. Singh, and S. S. Gill, "Fog computing: A taxonomy, systematic review, current trends and research challenges," *Journal of Parallel and Distributed Computing*, vol. 157, pp. 56–85, 2021.
7. C. Pu, "Sybil attack in rpl-based internet of things: analysis and defenses," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4937–4949, 2020.
8. W. W. Lo, S. Layeghy, M. Sarhan, M. Gallagher, and M. Portmann, "E-graphsage: A graph neural network based intrusion detection system for iot," in *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2022, pp. 1–9.
9. F. M. Ribeiro Junior, R. A. Bianchi, R. C. Prati, K. Kolehmainen, J.-P. Soininen, and C. A. Kamienski, "Data reduction based on machine learning algorithms for fog computing in iot smart agriculture," *Biosystems Engineering*, 2022.
10. P. Krishnan, S. Duttagupta, and K. Achuthan, "Sdn/nfv security framework for fog-to-things computing infrastructure," *Software: Practice and Experience*, vol. 50, no. 5, pp. 757–800, 2020.
11. J. Li, J. Jin, D. Yuan, and H. Zhang, "Virtual fog: A virtualization enabled fog computing framework for internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 121–131, 2017.
12. W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: a review," *Ieee Access*, vol. 6, pp. 10 179–10 188, 2018.
13. P. Kumar, R. Kumar, G. P. Gupta, and R. Tripathi, "A distributed framework for detecting ddos attacks in smart contract-based blockchain-iot systems by leveraging fog computing," *Transactions on Emerging Telecommunications Technologies*, p. e4112, 2020.
14. Y. I. Alzoubi, V. H. Osmanaj, A. Jaradat, and A. Al-Ahmad, "Fog computing security and privacy for the internet of thing applications: State-of-the-art," *Security and Privacy*, p. e145.
15. A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, "Ton˙iot telemetry dataset: A new generation dataset of iot and iiot for data-driven intrusion detection systems," *IEEE Access*, vol. 8, pp. 165 130–165 150, 2020.

Ahamed Aljuhani received the M.S. degree in computer science from the University of Colorado Denver, Denver, CO, USA, and the Ph.D. degree in computer science/information security track from The Catholic University of America, Washington, DC, USA. He is currently an Assistant Professor and the Chair of

the Department of Computer Engineering, College of Computing and Information Technology, University of Tabuk, Saudi Arabia. His current research interests include information security, network security and privacy, secure system design, and system development. Contact him at a_aljuhani@ut.edu.sa.

Prabhat Kumar received his Ph.D. degree in Information Technology from National Institute of Technology Raipur, Raipur, India, under the prestigious fellowship of Ministry of Human Resource and Development (MHRD) funded by the Government of India in 2022. Then, he worked with Indian Institute of Technology Hyderabad, India as a Post-Doctoral Researcher under project "Development of Indian Telecommunication Security Assurance Requirements for IoT devices". He is currently working as a Post-Doctoral Researcher with the Department of Software Engineering, LUT School of Engineering Science, LUT University, Lappeenranta, Finland. He has many research contributions in the area of Machine Learning, Deep Learning, Federated Learning, Big Data Analytics, Cybersecurity, Blockchain, Cloud Computing, Internet of Things and Software Defined Networking. He has authored or coauthored over 25+ publications in high-ranked SCI journals and conferences since 2019. Contact him at prabhat.kumar@lut.fi.

Randhir Kumar received his Ph.D. degree in Information Technology, National Institute of Technology Raipur, Raipur, India in 2021. He has published his research article in leading journal and conferences from IEEE, Elsevier, Springer, and John Wiley. He has published more than 40 research article in the reputed journals and conferences. His paper has been published in some of the high impact factor journals such as – IEEE Internet of Things, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Network Science and Engineering, IEEE Transactions on Green Communications and Networking, IEEE Transactions on Industrial Informatics, IEEE COMSNETs, IEEE ICC, Computer Networks, JPDC, and Transactions on Emerging Telecommunications Technologies (ETT Wiley). His research interest includes cryptographic techniques, information security, blockchain technology, and web mining. He is also an IEEE Member. Contact him at randhir.honeywell@ieee.org.

Alireza Jolfaei is an Associate Professor of Networking and Cyber Security in the College of Science and Engineering at Flinders University, Adelaide, Australia. He is a Senior Member of the IEEE and a Distinguished Speaker of the ACM. His main research interest is in Cyber-Physical Systems Security. He has published over 100 papers, which appeared in peer-reviewed journals, conference proceedings, and books. Before Flinders University, he has been a faculty member with Macquarie University, Federation University, and Temple University in Philadelphia, PA, USA. He received the prestigious IEEE Australian council award for his research paper published in the IEEE Transactions on Information Forensics and Security. He has served as a program co-Chair, a track Chair, a session Chair, and a Technical Program Committee member, for major conferences, including IEEE TrustCom and IEEE ICCCN. Contact him at alireza.jolfaei@flinders.edu.au.

A.K.M Najmul Islam is an Associate Professor at Software Engineering, LUT University, Finland. He is an adjunct professor of Information Systems at Tampere University, Finland. He has received his PhD from the University of Turku, Finland, and M.Sc. from Tampere University of Technology, Finland. He has published in other highly ranked journals such as IEEE Transactions on Industrial Informatics (TII), IEEE Transactions on Artificial Intelligence, IEEE Access, Computers in Industry, Computers & Education, Journal of Strategic Information Systems, European Journal of Information Systems and Information Systems Journal, Technological Forecasting and Social Change, International Journal of Information Management, Information Technology & People, Computers in Human Behavior, Internet Research, Communications of the AIS, among others. He is currently serving as a Senior Editor for Information Technology & People journal. Contact him at najmul.islam@lut.fi.