2020 IEEE 14th International Conference on Application of Information and Communication Technologies (AICT) | 978-1-7281-7386-3/20/$31.00 ©2020 IEEE | DOI: 10.1109/AICT50176.2020.9368580

Towards Secured Service Provisioning for the Internet of Healthcare Things

Fahiba Farhin
Institute of Information Technology
Jahangirngar Univesity,
Savar, 1342 – Dhaka, Bangladesh
farhinfahiba@gmail.com
ORCID: 0000-0002-5106-3461

M. Shamim Kaiser
Institute of Information Technology
Jahangirnagar University
Savar, 1342 – Dhaka, Bangladesh
mskaiser@juniv.edu
ORCID: 0000-0002-4604-5461

Mufti Mahmud
Department of Computing & Technology
Nottingham Trent University
Clifton, NG11 8NS – Nottingham, UK
mufti.mahmud@ntu.ac.uk
ORCID: 0000-0002-2037-8348

***Abstract*—The Internet of Healthcare Things (IoHT) is an emerging intelligent pervasive framework that interconnects smart healthcare devices, stakeholders (e.g., doctors, patients, researchers, healthcare professionals, etc.), and infrastructure using smart sensors. Emergence of novel tools and techniques for data sensing and analysis during the last decade have allowed many researchers to develop and deliver services tailored for the IoHT. This resulted in a considerable number of research outcomes addressing the applications, challenges, and probable solutions targeting secured communication within the IoHT framework. Despite considerable efforts dedicated to it, secured service provisioning still remains as a major challenge. This work provides a detailed account on the current challenges and solutions towards providing secured service provisioning focusing on the IoHT attacks and countermeasures with an aim to facilitate more investigation in this area.**

***Index Terms*—Internet of things (IoT), data analytics, software defined network (SDN), blockchain, data fusion, 5G network**

I. Introduction

The Internet of Things or commonly known as IoT includes things (such as, objects, devices, infrastructure, etc.) connected to embedded devices via smart sensors. These embedded devices connects those smart sensors to the Internet. Thus IoT is considered as an integrated part of the future internet. In recent years, IoT has drawn considerable attention to the research communication and it provided solutions for smart cities, agriculture, industry, office, automobile, retails, security services, and healthcare [1].

Given that IoT related research has sharply grown over the last years in diverse domains, many interdisciplinary research have been carried out within the healthcare setting. The Internet of Healthcare Things (IoHT) integrates healthcare devices (e.g., imaging devices, physiological sensing devices, diagnostic devices, patient tracking, real time patient monitoring at home/hospital, etc.), infrastructure (e.g., ambulance, wheelchair, bed, pharmacy, billing, etc.) and services (e.g., elderly care, fitness, remote monitoring, and personalised treatment delivery, etc.) enabled by the IoT [2], [3]. The aims of IoHT are reducing healthcare cost and device downtime, enhancing the user experience, and improving quality of life by optimizing the utilization of healthcare resources.

Joel *et al.* presents a review of enabling technologies for the IoHT and shows state-of-the-art of e-healthcare fields analyzing the challenges and trends [4]. The work by Mahmoud *et al.* focuses on the integration of cloud computing and the IoT which results in the Cloud of Things (CoT) within the context of smart healthcare systems that includes CoT concepts, architectures, platforms and applications in e-healthcare [5]. Large number of patient data is collected in hospitals using medical devices, including vital signs can be handled using IoHT to provide better diagnosis and patient care [6].

There exist numerous challenges and threats within the various aspects of IoHT ecosystem. This has been discussed in various research from architecture and applications perspectives focusing commonly on data management, interoperability, regulations, human-device-network interactions, and scalability [7]. Among the challenges, privacy and security are the two main issues in IoHT frameworks as it is expected to provide services any-time, any-where, and any-medium [2]. Hathaliya *et al.* provides an exhaustive survey to maintain security and privacy in e-Healthcare [8], while Kang *et al.* provides a systematic review of the current protocols for security implementation of IoHT in mobile health networks [9]. Various systems have been proposed to ensure healthcare data security including cryptographic encryption based hybrid optimization for medical image security in the electronic Health record (eHR) [10], machine learning-based security framework to detect malicious activities in a smart healthcare system [11], secure service oriented architecture for collaborative biosignal analysis research [12], and secured healthcare application in neuroscience domain [13].

Despite the extensive effort exerted into the research on privacy and security for the IoHT frameworks, it is still in its infancy. To facilitate integration of security and privacy, this work discusses an IoHT framework with five layers, and provides a comprehensive review on privacy and security issues in those layers. The work anticipates layer-wise attacks and accordingly discusses countermeasures and finally, main challenges and solutions are outlined at the end.

The rest of the paper describes the five layer IoHT framework in Section II and lists various attacks and corresponding countermeasures in section III along with challenges and some possible future work. The work is concluded in section IV.

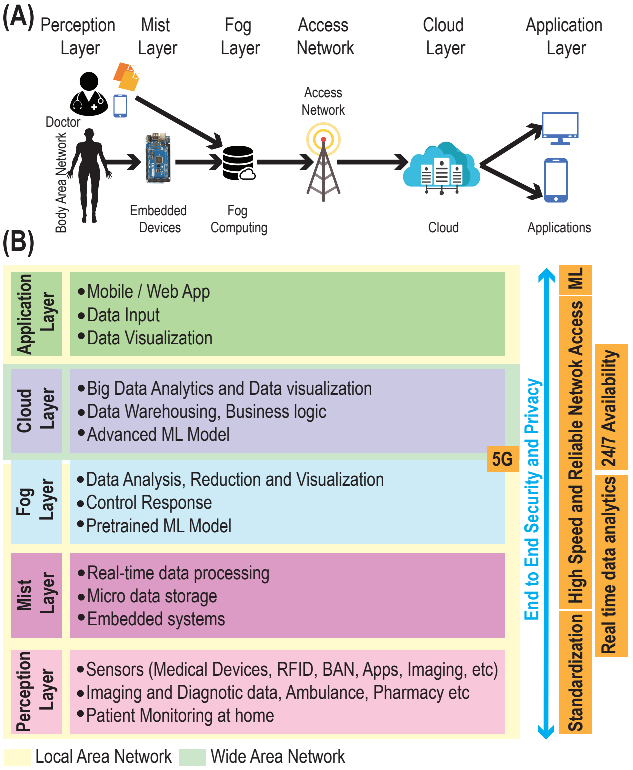


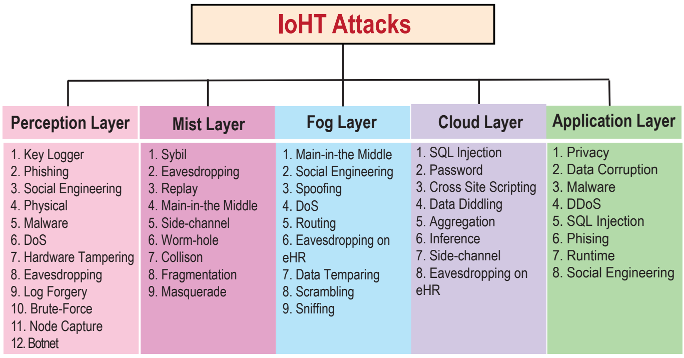
Fig. 1. (A) An exemplary scenario of the IoHT framework. (B) Different layers and functions of each layer within the IoHT framework. It contains five layers– Perception, Mist, Fog, Cloud, and Application. While the perception layer senses data, the rule based data processing is performed in the Mist layer, data reduction and real time data analysis can be done in Fog Layer and advanced data analytics can be performed in Cloud Layer. All the challenges are pointed out on the right side of the figure.

II. Internet of Healthcare Things and Relevant Security Attacks

IoHT connects peoples, devices, infrastructure in a hospital and patient in a home using sensors, computing devices and software where these nodes can interact, collect and exchange data. To ensure better quality of experience and low power consumption, an IoHT framework containing five layers, namely, Perception, Mist, Fog, Cloud, and Application has been proposed (see Fig. 1). Detailed discussion on this framework has been discussed in [2]. Such generic IoHT frameworks face various challenges including security and privacy threats at devices and infrastructure levels, and lack of standardization in healthcare big data. The relevant threats and attacks along with their layer-wise taxonomy for the IoHT framework have been investigated and listed in Fig. 2. Also, Table I depicts existing solutions for mitigating these attacks.

A. Perception Layer

The perception layer includes people, medical devices and hospital infrastructure and collects healthcare data [2]. The perception layer is vulnerable and the common attacks at perception layers are – keylogger, physical, hardware tampering, node capture whereas malware, DoS, eavesdropping, brute-force, botnet and social engineering, phishing, and log-forgery.



Perception Layer	Mist Layer	Fog Layer	Cloud Layer	Application Layer
1. Key Logger	1. Sybil	1. Main-in-the Middle	1. SQL Injection	1. Privacy
2. Phishing	2. Eavesdropping	2. Social Engineering	2. Password	2. Data Corruption
3. Social Engineering	3. Replay	3. Spoofing	3. Cross Site Scripting	3. Malware
4. Physical	4. Main-in-the Middle	4. DoS	4. Data Diddling	4. DDoS
5. Malware	5. Side-channel	5. Routing	5. Aggregation	5. SQL Injection
6. DoS	6. Worm-hole	6. Eavesdropping on eHR	6. Inference	6. Phising
7. Hardware Tampering	7. Collison	7. Data Temparing	7. Side-channel	7. Runtime
8. Eavesdropping	8. Fragmentation	8. Scrambling	8. Eavesdropping on eHR	8. Social Engineering
9. Log Forgery	9. Masquerade	9. Sniffing		
10. Brute-Force				
11. Node Capture				
12. Botnet				

Fig. 2. Taxonomy of attacks on different layers of the IoHT framework.

B. Mist Layer

Mist layer performs rule-based preprocessing of the data received from the perception layer to facilitate real-time data handling and to ensure resource optimization. It works as a pathway between physical device and fog layer which contains micro data storage and embedded systems. Therefore, malicious activities by hackers can affect communication devices and/or network. Common attacks in this layer include– Sybil, eavesdropping, replay, man-in-the-middle, side-channel, worm-hole, collision, fragmentation, and masquerade.

C. Fog Layer

In conventional and secured cloud computing based ecosystems, storage and processing at the cloud take time and result in latency and power consumption issues. To solve these, the fog layer is introduced which adds smart IoT-Fog gateway to facilitate reliability and improved performance. It processes data 'on the fly' to generate real-time alerts and automatically control responses. Advanced tools are used for data visualization and reduction, with pre-trained machine learning (ML) models for anomaly detection. Abnormalities or anomalies affects fog layer through attacks like– pharming and dumpster diving which is a kind of social engineering, man-in-the-middle, spoofing, Denial-of-service (DoS), routing, eavesdropping, data-tampering, scrambling, and sniffing.

D. Cloud Layer

Processed heterogeneous healthcare data coming from the fog layers are stored in the cloud. It also performs various advanced data analytics. Given that ML has attracted much attention and has successfully been applied to various tasks such as, anomaly detection [14]–[17], biological data mining [18], [19], disease detection [20]–[28], elderly monitoring [29]–[31], financial forecasting [32], image analysis [33], [34],natural language processing [35], [36], patient monitoring [37], [38]. Artificially intelligent, ML and reasoning-based algorithms are employed in the cloud for data analysis. Attacks in the cloud layer includes– SQL injection, password stealing, cross-site scripting, data diddling, weak-authentication, targeted data mining, aggregation, inference, and eavesdropping.

TABLE I
ATTACKS AND COUNTERMEASURE ON IOHT ARCHITECTURE

Attack	Layer	Description	Countermeasure	Ref.
Keylogger	P	Malicious software steal credential and sensitive information	Anti keyloggers; Anti-spyware; Network monitors; OTP	[39] [40]
Phishing	P	An attacker gains access to sensitive and confidential hospital and eHR information via email/phone	Augmented password login, Filters, 2-factor authentication; Attack profile modeling	[41], [42]
SocialEngg	P, F, A	Psychological manipulation trick for users to initiate security mistakes or disclosing sensitive information	Backup; Awareness; Tamper proofing; Multifactor authentication	[43] [44]
Physical	P	Attacks on sensor/hardware components	Energy auditing; Monitoring, Trust Model	[45]
Malware	P, A	Install malicious software and gain access to personal information or damage the device	Backup; Up-to-date software, Scan executable files.	[9]
DoS	P, F, A	Attacker overloads target machine/network resource and disrupts services unavailable to legitimate users .	Blowfish; Meta-heuristic; Traceback; AES; Cuckoo search; DistBlockNet; Bio-inspired; Trust Model; DL; Blockchain.	[8], [46]–[49]
HardTamp	P	Gain physical access and altered/replaced with an attacker node to obtain sensitive information.	Protecting the physical package.	[9]
Eavesdropping	P, M, F, C	Malicious user accesses the network and breach the personal privacy/confidential information.	Shielding; Filtering; Jamming and Source location privacy; Trust Model	[50], [51]
Log Forgery	P	Input un-trusted/un-validated data in log files and intended to ultimately corrupt the file.	Validation at server and client's end; Scrutinizing; Authentication.	[52]
Brute-Force	P	Intended to get personal information such as passwords or PIN using automated software.	Lockout mechanisms; Site scanners; AES/DES; blowfish; RC6; IDEA.	[49], [53]
Node Capture	P	Captures node(s) to compromise tag information, clones the tag to bypass security measures and copy all data.	Key management scheme.	[49]
Botnet	P	Attackers control botnet by malware and leaks credentials and may initiate DDoS attacks	ML based network anomaly detection	[54]
Sybil	M	Attackers unsettle the network service by presenting different identities and uses them to gain control	Authentication (e.g., Blockchain); Position verification; and Trust model.	[46], [49]
Replay	P	Attacker sents a request to a server at a later time after sniffing ongoing sessions and credentials.	Blockchain; Triangle-based security; Firmware update.	[8], [55]
MITM	M, F	A eavesdropping/hijacking attack where an attacker inserts a relay/proxy into a session and collects transfer of data.	EXCHANge protocol; Secured MQTT; Entity authentication; IPS IDS	[56], [57]
Side-Ch	M, C	An attacker breaks security mechanisms by inspecting side-channel information such as software bug/cyptoanalysis.	Spy Detector; CloudRadar; Blocking; Isolation; tamper-proofing; obfuscating; Firewall; Random cryptography.	[58]–[60]
Wormhole	M	A malicious node capture packets from a position in the network and tunneled these to another malicious node at a distance place.	Packet leashes authentication; Fuzzy; SHA algorithm; MapReduce	[48], [49]
Collision	M	A hash collision occurs when 2 inputs produce same hash value.	Data rate limit; Short frames; Error-correcting code	[9], [61]
Fragmentation	M	IP fragmentation attack is a special type of DoS attack, in which attackers access a network by using datagram fragmentation	New fields to fragmentation header; content change; Split buffer approach	[62]
Masquerade	M	Using stolen credential, an attacker employs a fake ID to access healthcare system and received privileges like a legitimate user.	Efficient, cost-effective middle-ware solution	[63]
Spoofing	F	A malicious user pretends as legitimate user, and initiates attack(s) to steal data, passes malware or escapes access controls.	Authentication;DEMOTE scheme Link-layer encryption.	[49], [64]
Routing	F	An attacker spoofs redirects, or drop the packets at the communication level by changing routing information	Link-layer encryption, Authentication,SVELTE IDS	[9], [65]
DataTamp	F	An attacker enters the system as a legitimate user and alter the e-HR data for ransomware	Network scanning; Firewall; HSAM, TamperProof	[66], [67]
Scrambling	F	A jamming attack disrupts the services for a specific interval	Profile Differentiation	[68]
Sniffing	F	Sniffing attack corresponds to the data theft or interception by capturing the network traffic using a sniffer.	Secure Certificate Public Key; Nagle's Algorithm.	[69]
SQLInj	C, A	Attack is initiated to the eHR connected to a app by inserting a malformed SQL statement and compromise eHR data	ML analytic; Hashing; SQLrand; Anomaly detection	[53], [70]
CrSScript	C	Malicious scripts are injected into trusted websites	Content Security Policy; Filtering; XSS mechanisms.	[71]
DataDidd	C	An attacker gains access to the eHR and changes the information.	VPN encryption; Auditing; ML based prevention	[72]
Aggregation	C	Aggregation attack collects small pieces of insensitive information and aggregate them them to estimate sensitive information.	Tree-based and cluster-based data aggregation protocols.	[73]
Inference	C	An Inference Attack illegitimately gain knowledge about eHR by analyzing healthcare data.	Multiple mitigation framework; Collective Data-sensitization.	[74]–[76]
Privacy	A	Attackers explore behavioral and social relation, and infer such data for criminal activities or sold for marketing purposes.	Profile matching protocol; Pseudonyms; Attribute-based method.	[77], [78]
DataCorr	A	An attacker can disturb the communication channel between two IoT nodes by corrupting transmitted heath data, and may result a DoS attack.	Minos systems; Pointer taintedness architecture.	[79], [80]
Runtime	A	An attacker intercepts or alters critical information by unauthorized access and breaching the privacy and availability of the resources which can cause devastating data loss	Cryptographic API, Modifications to current standards, Reduction of functionalities.	[81]

Legend: *On Layer Column:* P–Physical layer; M–Mist layer; F–Fog layer; C–Cloud layer; A–Application Layer. *On Attack Column:* SocialEngg–Social Engineering; HardTamp–Hardware Tampering; MITM–Man-in-the-Middle; Side-Ch–Side-Channel; DataTamp–Data Tampering; CrSScript–Cross Site Scripting; SQLInj–SQL Injection; DataDidd–Data Diddling; DataCorr–Data Corruption. *On Description column:* OTP–One time password; DL– Deep learning

E. Application Layer

Application layer provides shared communication protocols and services along with various interface methods between the end users, stakeholders and communications network. As the application layer employs various programs and applications, to perform exchange of messages, to provide access to various services, and to access files and manage them. This layer is more susceptible to attacks due to the fact that many end users are not properly trained to detect the attacks. The main vulnerabilities in the cloud layer include– privacy theft, data corruption, malware, large overhead resulting DDoS, SQL injection, phishing, and social engineering attack, etc.

III. Current Challenges and Research Directions

Though there has been a significant amount of effort among the interdisciplinary researchers to make the IoHT frameworks more secure and tackle the possible threats, attacks and vulnerabilities, there still remain many challenges to be addressed in the future. Some of these challenges are outlined in the following sections.

A. Data Interoperability

Data Interoperability may create trouble in identifying patients in situations where eHRs come from diverse sources. This problem is particularly important in the context of today's globalized world and free movement - especially when there are situations such as pandemics. This problem may be solved by using a unique global ID for each patient. Though Blockchain can ensure security in identifying patient record in the eHR, yet, this remains an open challenge in the field [82].

B. Heterogeneous Data Fusion

Heterogeneous data collected using multiple sensors to denote different health parameters can provide true insights. However, the fusion of such heterogeneous data is very challenging. At the sensor level, various sensors are sensitive to various physical quantity and generate different aspects with different units. At the data level, the size alignment and resolution of multi-sensor data are different, and also, data may be noisy, unbalanced, inconsistent, and contain missing data. At the model design level, the selection of proper fusion rule and data can be fused not only at the low level (e.g., fusion of raw data) which can give the best inference but also at a high level (e.g., knowledge) which is easier to handle [83].

C. Real-time Data Processing

For many healthcare applications, real-time data analysis is very important and may be life saving. In traditional settings, many of the existing frameworks cannot handle both conventional and real-time data sources [7]. In recent years there have been a few frameworks to accommodate this, however, they are still in prototype levels. For many time-sensitive applications real-time data cannot be processed in the cloud layer due to the high propagation delay. With the advent of 5G access network, researchers are working on streaming and batch processing to process the data in cloud in near real time [2].

D. 5G Wireless Core

The IoHT framework often connects many bandwidth-hungry medical devices requiring real-time data processing and data access with ultra-low latency. The 5G wireless core can support connectivity to higher number of devices with high bandwidth and low latency. Besides, it can enable rapid access of patient data, creation of reliable telemedicine services, and monitoring of remote patients. The challenges of such a system are high absorption ratio when obstructed by buildings, trees, etc, high rollout cost, high maintenance cost and concerned about the high-frequency radiation on human body for extended time [84].

E. Software Defined Network and Blockchain

Security and privacy are the two main concerns of the next generation IoHT frameworks. The system aims to ensure 24/7 data availability at anytime and anywhere which increases these concerns. However, devices with strong security features and network monitoring capabilities to find threats and abnormalities, centralized and distributed security measures may help to reduce security and privacy concerns. In recent days, researchers are working on Blockchain, software defined network (SDN) and network function virtualization (NFV) in IoHT settings. Blockchain is transparent, immutable and distributed where data is stored cryptographically inside. However, public blockchain is impractical to use in the healthcare settings due to its low storage, limited transaction (7 to 8) per second, and high confirmation latency. Thus, there is a scope to design ecosystem for the private chains which will ensure low confirmation latency, high storage, high privacy, and security. Besides, SDN with NFV can also be used to detect abnormalities in the distributed IoHT networks, and taken necessary countermeasures [85].

F. Deep Machine Learning

Deep Machine Learning (DML) models are gaining increased popularity in predicting models for disease diagnosis, prognosis, drug design, and risk analysis. Besides, DML is extensively used in monitoring malicious activity, real-time anomaly detection, self-healing of healthcare networks and repetitive security tasks. It is still a challenge to develop models which will integrate diverse data types and run on different machines. Also, there is the problem of these models requiring large amount of data for training and the models' outputs are often obscure [18].

G. Secure Big data Analytics

The cloud platform can facilitate the extensive data analytics by providing a large amount of storage, ML-based data mining, and analytic tools to find valuable insights from the data. However, these types of frameworks (e.g., Hadoop and Mapreduce) are difficult to setup and maintain. The platforms may be manifested privacy breaches and data leakage threats. Homomorphic encryption-based big data analytic for cloud-led applications is proposed in [86], [87] which might lead to greater latencies.

IV. Conclusion

The development of IoHT frameworks has interconnected heterogeneous smart objects, and ensure anywhere, anytime and anything connectivity in the healthcare settings. Researchers have come up with a lot of proposals which will improve the service provisioning of these frameworks. In this work, we surveyed IoHT attacks and countermeasures, their challenges, and possible solutions aiming to reduce healthcare cost and device downtime, enhancing the user experience, and improving quality of life by utilizing limited healthcare resources. This work can be further extended by incorporating Machine learning and distributed security to detect and prevent layer-wise IoHT attacks.

References

[1] F. Firouzi, B. Farahani, M. Ibrahim, and K. Chakrabarty, “Keynote Paper: From EDA to IoT eHealth: Promises, Challenges, and Solutions,” *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 37, no. 12, pp. 2965–2978, Dec. 2018.

[2] M. Asif-Ur-Rahman and et al., “Toward a heterogeneous mist, fog, and cloud-based framework for the internet of healthcare things,” *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4049–4062, 2019.

[3] F. Farhin, I. Sultana, N. Islam, M. S. Kaiser, M. S. Rahman, and M. Mahmud, “Attack detection in internet of things using software defined network and fuzzy neural network,” in *Proc. ICIEV*. IEEE, 2020, pp. 1–6.

[4] J. J. P. C. Rodrigues and et al., “Enabling technologies for the internet of health things,” *IEEE Access*, vol. 6, pp. 13 129–13 141, 2018.

[5] M. M. E. Mahmoud *et al.*, “Enabling technologies on cloud of things for smart healthcare,” *IEEE Access*, vol. 6, pp. 31 950–31 967, 2018.

[6] da Costa et al., “Ioht: Toward intelligent vital signs monitoring in hospital wards,” *Artif. intell. med.*, vol. 89, pp. 61–69, 2018.

[7] B. Farahani and et al., “Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare,” *Future Gener. Comput. Syst.*, vol. 78, pp. 659–676, Jan. 2018.

[8] J. J. Hathaliya and S. Tanwar, “An exhaustive survey on security and privacy issues in healthcare 4.0,” *Computer Communications*, 2020.

[9] J. J. Kang, “Systematic analysis of security implementation for internet of health things in mobile health networks,” in *Data Science in Cybersecurity and Cyberthreat Intelligence*. Springer, 2020, pp. 87–113.

[10] M. Elhoseny, K. Shankar, S. Lakshmanaprabu, A. Maseleno, and N. Arunkumar, “Hybrid optimization with cryptography encryption for medical image security in internet of things,” *Neural comput. appl.*, pp. 1–15, 2018.

[11] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, “HealthGuard: A Machine Learning-Based Security Framework for Smart Healthcare Systems,” in *2019 SNAMS*, Oct. 2019, pp. 389–396.

[12] M. Mahmud, M. M. Rahman, D. Travalin, P. Raif, and A. Hussain, “Service oriented architecture based web application model for collaborative biomedical signal analysis,” *Biomed. Tech. (Berl)*, vol. 57, no. SI-1 Track-N, pp. 780–783, 2012.

[13] M. Mahmud, M. S. Kaiser, M. M. Rahman, M. A. Rahman, A. Shabut, S. Al-Mamun, and A. Hussain, “A brain-inspired trust management model to assure security in a cloud based iot framework for neuroscience applications,” *Cognitive Computation*, vol. 10, no. 5, pp. 864–873, 2018.

[14] S. W. Yahaya, A. Lotfi, and M. Mahmud, “A consensus novelty detection ensemble approach for anomaly detection in activities of daily living,” *Appl. Soft Comput.*, vol. 83, p. 105613, 2019.

[15] “Neural network-based artifact detection in local field potentials recorded from chronically implanted neural probes,” in *Proc. IJCNN*, 2020, pp. 1–8.

[16] M. Fabietti, M. Mahmud, and A. Lotfi, “Effectiveness of Employing Multimodal Signals in Removing Artifacts from Neuronal Signals: An Empirical Analysis,” in *Brain Informatics*, ser. Lecture Notes in Computer Science, M. Mahmud, S. Vassanelli, M. S. Kaiser, and N. Zhong, Eds. Cham, Switzerland: Springer, 2020, pp. 183–193.

[17] ——, “Machine Learning in Analysing Invasively Recorded Neuronal Signals: Available Open Access Data Sources,” in *Brain Informatics*, M. Mahmud, S. Vassanelli, M. S. Kaiser, and N. Zhong, Eds. Cham, Switzerland: Springer, 2020, pp. 151–162.

[18] M. Mahmud, M. S. Kaiser, A. Hussain, and S. Vassanelli, “Applications of deep learning and reinforcement learning to biological data,” *IEEE trans. neural netw. learn. syst.*, vol. 29, no. 6, pp. 2063–2079, 2018.

[19] M. Mahmud, M. S. Kaiser, T. M. McGinnity, and A. Hussain, “Deep Learning in Mining Biological Data,” *arXiv:2003.00108 [cs, q-bio, stat]*, vol. abs/2003.00108, pp. 1–36, Feb. 2020.

[20] M. B. T. Noor, N. Z. Zenia, M. S. Kaiser, M. Mahmud, and S. Al Mamun, “Detecting neurodegenerative disease from mri: A brief review on a deep learning perspective,” in *Proc. Brain Informatics*. Springer, 2019, pp. 115–125.

[21] Y. Miah, C. N. E. Prima, S. J. Seema, M. Mahmud, and M. S. Kaiser, “Performance comparison of machine learning techniques in identifying dementia from open access clinical datasets,” in *Proc. ICACIn*. Springer, Singapore, 2020, pp. 69–78.

[22] M. F. Zohora, M. H. Tania, M. S. Kaiser, and M. Mahmud, “Forecasting the risk of type ii diabetes usingreinforcement learning,” in *Proc. ICIEV*. IEEE, 2020, pp. 1–6.

[23] R. Sharpe and M. Mahmud, “Effect of the Gamma Entrainment Frequency in Pertinence to Mood, Memory and Cognition,” in *Brain Informatics*, M. Mahmud, S. Vassanelli, M. S. Kaiser, and N. Zhong, Eds. Cham, Switzerland: Springer, 2020, pp. 50–61.

[24] M. S. Satu, S. Rahman, M. I. Khan, M. Z. Abedin, M. S. Kaiser, and M. Mahmud, “Towards Improved Detection of Cognitive Performance Using Bidirectional Multilayer Long-Short Term Memory Neural Network,” in *Brain Informatics*, M. Mahmud, S. Vassanelli, M. S. Kaiser, and N. Zhong, Eds. Cham, Switzerland: Springer, 2020, pp. 297–306.

[25] S. Rahman, T. Sharma, and M. Mahmud, “Improving Alcoholism Diagnosis: Comparing Instance-Based Classifiers Against Neural Networks for Classifying EEG Signal,” in *Brain Informatics*, M. Mahmud, S. Vassanelli, M. S. Kaiser, and N. Zhong, Eds. Cham, Switzerland: Springer, 2020, pp. 239–250.

[26] M. B. T. Noor, N. Z. Zenia, M. S. Kaiser, S. Al Mamun, and M. Mahmud, “Application of deep learning in detecting neurological disorders from magnetic resonance images: A survey on the detection of alzheimer’s disease, parkinson’s disease and schizophrenia,” *Brain Informatics*, pp. 1–30, 2020, [Online First].

[27] V. M. Aradhya, M. Mahmud, D. Guru, B. Agarwal, and M. S. Kaiser, “One shot cluster based approach for the detection of covid-19 from chest x-ray images,” *Cogn Comput*, pp. 1–8, 2020, [ePub ahead of Print].

[28] N. Dey, V. Rajinikanth, S. J. Fong, M. S. Kaiser, and M. Mahmud, “Social group optimization–assisted kapur’s entropy and morphological segmentation for automated detection of covid-19 infection from computed tomography images,” *Cogn Comput*, vol. 12, no. 5, pp. 1011–1023, 2020.

[29] M. J. Al Nahian, T. Ghosh, M. N. Uddin, M. M. Islam, M. Mahmud, and M. S. Kaiser, “Towards Artificial Intelligence Driven Emotion Aware Fall Monitoring Framework Suitable for Elderly People with Neurological Disorder,” in *Brain Informatics*, M. Mahmud, S. Vassanelli, M. S. Kaiser, and N. Zhong, Eds. Cham, Switzerland: Springer, 2020, pp. 275–286.

[30] S. Jesmin, M. S. Kaiser, and M. Mahmud, “Artificial and Internet of Healthcare Things Based Alzheimer Care During COVID 19,” in *Brain Informatics*, M. Mahmud, S. Vassanelli, M. S. Kaiser, and N. Zhong, Eds. Cham, Switzerland: Springer, 2020, pp. 263–274.

[31] M. Nahiduzzaman, M. Tasnim, N. T. Newaz, M. S. Kaiser, and M. Mahmud, “Machine Learning Based Early Fall Detection for Elderly People with Neurological Disorder Using Multimodal Data Fusion,” in *Brain Informatics*, M. Mahmud, S. Vassanelli, M. S. Kaiser, and N. Zhong, Eds. Cham, Switzerland: Springer, 2020, pp. 204–214.

[32] O. Orojo, J. Tepper, T. M. McGinnity, and M. Mahmud, “A Multi-recurrent Network for Crude Oil Price Prediction,” in *Proc. IEEE SSCI*. IEEE, 2019, pp. 2953–2958.

[33] H. M. Ali, M. S. Kaiser, and M. Mahmud, “Application of convolutional neural network in segmenting brain regions from mri data,” in *Proc. Brain Informatics*. Springer, 2019, pp. 136–146.

[34] J. Ruiz, M. Mahmud, M. Modasshir, M. Shamim Kaiser, and f. t. Alzheimer’s Disease Neuroimaging Initiative, “3D DenseNet Ensemble in 4-Way Classification of Alzheimer’s Disease,” in *Brain Informatics*, M. Mahmud, S. Vassanelli, M. S. Kaiser, and N. Zhong, Eds. Cham, Switzerland: Springer, 2020, pp. 85–96.

[35] G. Rabby, S. Azad, M. Mahmud, K. Z. Zamli, and M. M. Rahman, “Teket: a tree-based unsupervised keyphrase extraction technique,” *Cogn. Comput.*, vol. 12, no. 4, pp. 811–833, 2020.

[36] J. Watkins, M. Fabietti, and M. Mahmud, “Sense: a student performance quantifier using sentiment analysis,” in *Proc. IJCNN*, 2020, pp. 1–6.

[37] M. H. Al Banna, T. Ghosh, K. A. Taher, M. S. Kaiser, and M. Mahmud, “A Monitoring System for Patients of Autism Spectrum Disorder Using Artificial Intelligence,” in *Brain Informatics*, M. Mahmud, S. Vassanelli, M. S. Kaiser, and N. Zhong, Eds. Cham, Switzerland: Springer, 2020, pp. 251–262.

[38] A. I. Sumi, M. F. Zohora, M. Mahjabeen, T. J. Faria, M. Mahmud, and M. S. Kaiser, “fassert: A fuzzy assistive system for children with autism using internet of things,” in *Brain Informatics*, S. Wang *et al.*, Eds. Cham, Switzerland: Springer, 2018, pp. 403–412.

[39] Wooguil Pak, Youngrok Cha, and Sunki Yeo, “High accessible virtual keyboards for preventing key-logging,” in *ICUFN*, 2016, pp. 205–207.

[40] M. Wazid and et al., “Implementation and Embellishment of Prevention of Keylogger Spyware Attacks,” in *Security in Computing and Communications*, ser. Communications in CIS, S. M. Thampi and et al., Eds. Springer, 2013, pp. 262–271.

[41] B. B. Gupta, N. A. G. Arachchilage, and K. E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," *Telecommun. Syst.*, vol. 67, no. 2, pp. 247–267, Feb. 2018.

[42] A. McLeod and D. Dolezel, "Cyber-analytics: Modeling factors associated with healthcare data breaches," *Decis. Support Syst.*, vol. 108, pp. 57–68, Apr. 2018.

[43] F. Salahdine and N. Kaabouch, "Social Engineering Attacks: A Survey," *Future Internet*, vol. 11, no. 4, p. 89, Apr. 2019, number: 4 Publisher: Multidisciplinary Digital Publishing Institute.

[44] N. Y. Conteh and P. J. Schmick, "Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks," *Int. J. Adv. Comput. Res.*, vol. 6, no. 23, pp. 31–38, Feb. 2016.

[45] F. Li, Y. Shi, A. Shinde, J. Ye, and W. Song, "Enhanced Cyber-Physical Security in Internet of Things Through Energy Auditing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5224–5231, Jun. 2019.

[46] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, Sep. 2017.

[47] G. Liu, W. Quan, N. Cheng, H. Zhang, and S. Yu, "Efficient DDoS attacks mitigation for stateful forwarding in Internet of Things," *J. Netw. Comput. Appl.*, vol. 130, pp. 1–13, Mar. 2019.

[48] R. Mehta and M. Parmar, "Trust based mechanism for Securing IoT Routing Protocol RPL against Wormhole Grayhole Attacks," in *2018 3rd I2CT*, Apr. 2018, pp. 1–6.

[49] S. N. Mahapatra, B. K. Singh, and V. Kumar, "A survey on secure transmission in internet of things: Taxonomy, recent techniques, research requirements, and challenges," *Arab. J. for Sci. and Eng.*, 2020.

[50] G. Han and et al., "CASLP: A Confused Arc-Based Source Location Privacy Protection Scheme in WSNs for IoT," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 42–47, Sep. 2018.

[51] M. E. S. Saeed, Q.-Y. Liu, G. Tian, B. Gao, and F. Li, "AKAIoTs: authenticated key agreement for Internet of Things," *Wirel. Netw.*, vol. 25, no. 6, pp. 3081–3101, Aug. 2019.

[52] N. Jovanovic, E. Kirda, and C. Kruegel, "Preventing Cross Site Request Forgery Attacks," in *2006 Securecomm and Workshops*, Aug. 2006, pp. 1–10.

[53] F. Alsubaei, A. Abuhussein, and S. G. Shiva, "Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment," *2017 IEEE LCN Workshops*, 2017.

[54] Y. Meidan and et al., "N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders," *IEEE Pervasive Comput.*, vol. 17, no. 3, pp. 12–22, Jul. 2018.

[55] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment," *J. Supercomput.*, vol. 73, no. 3, pp. 1152–1167, Mar. 2017.

[56] F. Aliyu, T. Sheltami, and E. M. Shakshuki, "A detection and prevention technique for man in the middle attack in fog computing," *Procedia Computer Science*, vol. 141, pp. 24–31, 2018.

[57] J. Partala and et al., "Security threats against the transmission chain of a medical health monitoring system," in *IEEE Healthcom 2013)*, Oct. 2013, pp. 243–248.

[58] T. Zhang, Y. Zhang, and R. B. Lee, "CloudRadar: A Real-Time Side-Channel Attack Detection System in Clouds," in *Research in Attacks, Intrusions, and Defenses*, ser. Lecture Notes in Computer Science. Cham: Springer, 2016, pp. 118–140.

[59] Y. Kulah, B. Dinçer, C. Yilmaz, and E. Savaş, "SpyDetector: An approach for detecting side-channel attacks at runtime," *Int. J. Inf. Secur.*, 2018.

[60] S. Singh, B. K. Pandey, R. Srivastava, N. Rawat, P. Rawat *et al.*, "Cloud computing attacks: a discussion with solutions," *Open Journal of Mobile Computing and Cloud Computing*, vol. 1, no. 1, pp. 1–10, 2014.

[61] N. Sharma and R. Bhatt, "Privacy Preservation in WSN for Healthcare Application," *Procedia Comput. Sci.*, vol. 132, pp. 1243–1252, Jan. 2018.

[62] R. Hummen and et al., "6lowpan fragmentation attacks and mitigation mechanisms," in *Proc. 6th ACM conference on Security and privacy in wireless and mobile networks*, 2013, pp. 55–66.

[63] N. Bruce, M. Sain, and H. J. Lee, "A support middleware solution for e-healthcare system security," in *16th ICACT*, Feb. 2014, pp. 44–47, iSSN: 1738-9445.

[64] S. Barman and et al., "A Secure Authentication Protocol for Multi-Server-Based E-Healthcare Using a Fuzzy Commitment Scheme," *IEEE Access*, vol. 7, pp. 12 557–12 574, 2019.

[65] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad Hoc Net.*, vol. 11, no. 8, pp. 2661–2674, Nov. 2013.

[66] N. Skrupsky, P. Bisht, T. Hinrichs, V. N. Venkatakrishnan, and L. Zuck, "TamperProof: a server-agnostic defense for parameter tampering attacks on web applications," in *Proc. ACM conf. DASP*, ser. CODASPY '13, Feb. 2013, pp. 129–140.

[67] A. Ahmed and et al., "Malicious insiders attack in IoT based Multi-Cloud e-Healthcare environment: A Systematic Literature Review," *Multimed. Tools Appl.*, vol. 77, no. 17, pp. 21 947–21 965, Sep. 2018.

[68] J. Jung, J. Jeung, and J. Lim, "Control channel hopping for avoidance of scrambling attacks in IEEE 802.16 systems," in *2011 - MILCOM*, Nov. 2011, pp. 1225–1230, iSSN: 2155-7586.

[69] B. Prabadevi and N. Jeyanthi, "A review on various sniffing attacks and its mitigation techniques," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 12, no. 3, pp. 1117–1125, 2018.

[70] W. G. J. Halfond and A. Orso, "AMNESIA: analysis and monitoring for NEutralizing SQL-injection attacks," in *ASE '05*, 2005.

[71] S. Gupta and B. B. Gupta, "Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art," *Int. J. Syst. Assur. Eng. Manag.*, vol. 8, no. 1, pp. 512–530, Jan. 2017.

[72] A. S. Choudhary, P. P. Choudhary, and S. Salve, "A Study On Various Cyber Attacks And A Proposed Intelligent System For Monitoring Such Attacks," in *2018 ICICT*, Nov. 2018, pp. 612–617.

[73] A. Sikarwar and K. Sharma, "A Survey on Data Aggregation Attacks and Approaches in Wireless Sensor Network," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 7, p. 227, Aug. 2017.

[74] T. H. Hinke, H. S. Delugach, and R. P. Wolf, "Protecting databases from inference attacks," *Computers & Security*, vol. 16, no. 8, pp. 687–708, Jan. 1997.

[75] J. Vaidya, B. Shafiq, X. Jiang, and L. Ohno-Machado, "Identifying inference attacks against healthcare data repositories," *AMIA Summits Transl. Sci. Proc.*, vol. 2013, pp. 262–266, 2013.

[76] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective Data-Sanitization for Preventing Sensitive Information Inference Attacks in Social Networks," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 4, pp. 577–590, Jul. 2018.

[77] L. Guo and et al., "PAAS: A Privacy-Preserving Attribute-Based Authentication System for eHealth Networks," in *2012 IEEE 32nd International Conference on Distributed Computing Systems*, Jun. 2012, pp. 224–233.

[78] S. Zeadally, J. T. Isaac, and Z. Baig, "Security Attacks and Solutions in Electronic Health (E-health) Systems," *J. Med. Syst.*, vol. 40, no. 12, p. 263, Oct. 2016.

[79] J. Crandall and F. Chong, "Minos: Control Data Attack Prevention Orthogonal to Memory Model," in *MICRO-37'04*, Dec. 2004, pp. 221–232, iSSN: 1072-4451.

[80] S. Chen, J. Xu, N. Nakka, Z. Kalbarczyk, and R. Iyer, "Defeating memory corruption attacks via pointer taintedness detection," in *DSN'05)*, Jun. 2005, pp. 378–387, iSSN: 2158-3927.

[81] R. Focardi and M. Squarcina, "Run-Time Attack Detection in Cryptographic APIs," in *2017 IEEE 30th CSF*, Aug. 2017, pp. 176–188, iSSN: 2374-8303.

[82] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, and S. W. Kim, "The future of healthcare internet of things: A survey of emerging technologies," *IEEE Communications Surveys Tutorials*, vol. 22, no. 2, pp. 1121–1167, 2020.

[83] M. S. Kaiser, K. T. Lwin, M. Mahmud, D. Hajializadeh, T. Chaipimonplin, A. Sarhan, and M. A. Hossain, "Advances in crowd analysis for urban applications through urban event detection," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 10, pp. 3092–3112, 2018.

[84] G. Cisotto, E. Casarin, and S. Tomasin, "Requirements and enablers of advanced healthcare services over future cellular systems," *IEEE Communications Magazine*, vol. 58, no. 3, pp. 76–81, 2020.

[85] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K. R. Choo, "An energy-efficient sdn controller architecture for iot networks with blockchain-based security," *IEEE Trans. Serv. Comput.*, pp. 1–14, 2020, doi: 10.1109/TSC.2020.2966970.

[86] A. Alabdulatif, I. Khalil, and X. Yi, "Towards secure big data analytic for cloud-enabled applications with fully homomorphic encryption," *J. Parallel Distrib. Comput.*, vol. 137, pp. 192 – 204, 2020.

[87] H. Kumarage, I. Khalil, A. Alabdulatif, Z. Tari, and X. Yi, "Secure data analytics for cloud-integrated internet of things applications," *IEEE Cloud Comput.*, vol. 3, no. 02, pp. 46–56, mar 2016.