IoT Security in Healthcare using AI: A Survey

Subiksha Srinivasa Gopalan[1], Dr Ali Raza[1], Dr Wesam Almobaideen[1,2]

[1]*Department of Electrical Engineering and Computing Sciences, Rochester Institute of Technology, Dubai, UAE*
[2]*Department of Computer Science, The University of Jordan, Amman, Jordan*
{ssg5920, axrcada, wxacad} @rit.edu, almobaideen@inf.ju.edu.jo

***Abstract*—Internet of Things (IoT) and Artificial Intelligence (AI) has led the digital transformation in modern healthcare. With any kind of digital transformation, security challenges must be considered in the early stages of the design. Healthcare data is sensitive and any breach compromises the privacy of patients. More so in IoT networks where the connected devices are vulnerable to attacks. Cyberattacks can result in life-threatening consequences. In this paper, a survey and analysis of research on the use of AI as a tool for cybersecurity to protect IoT networks used for healthcare are presented. A thorough analysis of literature between 2014 and 2019 is provided. A niche opportunity for researchers to focus on in this space is identified following a thorough analysis of related papers.**

Keywords—Internet of Things, Artificial Intelligence, Security, Privacy, Healthcare

I. Introduction

Technologies are rapidly advancing on a daily basis and they are made with a goal to make our lives easier. Healthcare industry has greatly benefitted from this technological advancement. It makes any long and tedious process easier to complete and allows doctors and medical personnel to use this amazing tool in a secure manner. Before technology was introduced in the healthcare industry, patients had to endure long waiting hours to get examined and staff had to complete tasks manually. Patients only interacted with the doctors through visits to the hospital, phone, and text. There was no way to monitor the patient's health continuously to make an immediate and accurate diagnosis. Internet of Things (IoT) and Artificial Intelligence (AI) in healthcare can help bring a tremendous change to medical analysis, disease diagnosis and patient care [1].

Internet of Things (IoT) is a network of physical devices that can connect and exchange information [2]. Information exchanged using connected IoT devices in healthcare is known as Internet of Medical Things (IoMT) [3]. Artificial Intelligence in healthcare is a technology that uses different software and algorithms to resemble human intelligence in order to process complex medical data and perform analysis, reasoning, pattern detection, carry out specific tasks and solve problems without any direct human interaction or input [4]. AI is a collection of different technologies. IoT devices used for healthcare can be in the form of wearables, biosensors or body sensors, and medical equipment. The collected medical data can be in the form of EHR, claims, patient registries, health surveys or clinical trial data [5]. AI is the most effective way to process all big data and make accurate analysis in real-time [6]. These technologies open new doors to exciting possibilities such as reducing doctor-patient visit, real-time monitoring of patients suffering from chronic illness, recovering patients, and bringing healthcare to rural areas.

Security is always an issue with any new technology and it's not different in this case. Cybersecurity breaches [7] of IoT device and medical data is a matter of life or death. Medical Equipment like a pacemaker, life support or oxygen supply system connected to the internet can vulnerable to different kinds of attacks and can leave a patient helpless. Connected IoT devices [8] in healthcare can pose risks to the security and privacy of the device, patient, and hospital.

A. Security and Types of Security

Security in terms of Information Technology (IT) is the protection of IT assets and digital information against threats [9]. The threats can be in the form of external, internal, accidental or malicious. The following are the types of security.

1) Physical Security: Physical Security deals with the protection of hardware, software, personnel, network and data from different kinds of threats such as physical actions, intrusions and inside events that could cause damage to an organization [9] .

2) Information Security: Information Security (Infosec) consists of a wide range of strategies to detect, prevent and respond to threats [10]. Infosec programs are based on 3 main objectives- CIA Triad i.e. Confidentiality, Integrity, Availability [11]. Infosec is a central part of Cybersecurity. Information Security consists of specialized categories that is represented in Figure 1.

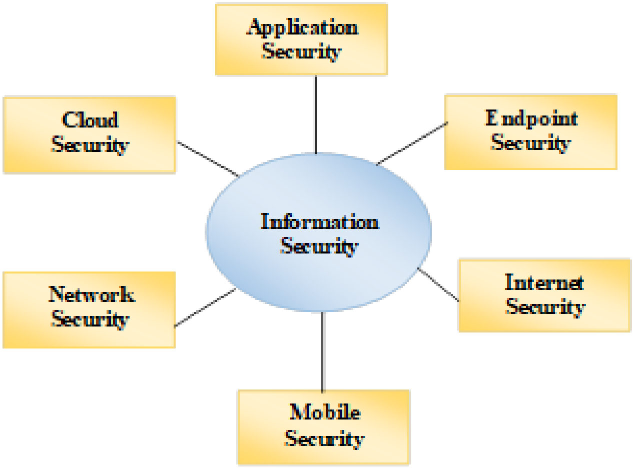

Fig. 1. Information Security categorization [9][12][13]

978-1-7281-6535-6/20/$31.00 ©2020 IEEE

B. *Contributions*

- A survey of related papers from the year 2014 to 2019.
- Tabulated form summarization of IoT security issues, frameworks, types of security and AI methods/techniques to assist these frameworks.
- Analysis and observation of these tables to highlight how AI can be used to tackle IoT security issues for different healthcare scenarios.

II. Related Survey Papers

Related Survey papers from the year 2014-2019 are collected and classified to analyze the different security issues of Internet of Things in the healthcare industry and how AI can be applied to resolve those issues. The type of security is classified based on the above-mentioned types. Table 1 can also be used to find what other technologies can be combined with AI to further enhance the security of IoT.

TABLE I. Summary of related survey papers

Paper Ref	Contributions	Technology/Techniques	Type of Security	Security Issues	Industry
[14]	A comprehensive discussion on the potential vulnerabilities and attack surfaces of the IoT system. In-depth review of Machine Learning (ML) and recent advances in Deep Learning (DL) methods for IoT security Application of ML/DL for each IoT layer, challenges, and future directions.	IoT, Machine Learning, Deep Learning, Big Data	Application and Network Security	Security measures like encryption, authentication, access control, network and application security for IoT devices and their inherent vulnerabilities are ineffective. Existing security methods need to be enhanced to secure the IoT ecosystem effectively.	All Industries
[15]	Extensive Survey on different cloud-based IoT HC systems that use Machine Learning for analyzing data. Review of different ML approaches used in cybersecurity A Standard model is proposed.	IoT, Cloud, Machine Learning	Information Security	Gathering and processing of large amounts of data from wearable sensors can cause many security issues for cloud-based IoT healthcare systems.	Healthcare
[16]	An in-depth systematic and comprehensive survey of the role of Machine Learning and Deep Learning in IoT. State of the art results on ML/DL that focuses on privacy and security of IoT Networks. Limitations of existing IoT network security solutions that call for DL and ML techniques. In-depth review of the research challenges of ML/DL techniques in IoT	IoT, Machine Learning, Deep Learning	Network Security	Unique characteristics of IoT render existing solutions insufficient because of resource constraints, heterogeneity, massive real-time data generated by IoT devices and the dynamic behavior of the networks.	All Industries

Table I provides a summary of all related survey papers. [14] discusses the various kinds of security threats in the IoT system and provides an in-depth review of machine learning and deep learning methods. IoT security in healthcare faces a challenge between availability and safety. This challenge can be mitigated with the help of ML and DL methods. Processing large amounts of data generated by IoT devices using the cloud in a secure manner can be a problem, In order to solve this problem, a solution of combining machine learning combined with healthcare IoT and cloud is proposed in [15]. A generic architecture is proposed to secure data transmission for analysis and detection of suspicious activities using cryptography and steganography. The architecture does not explain how ML/DL can be implemented [15]. Current security solutions for IoT networks and gaps in the security solution that calls for machine and deep learning are reviewed in [16].

Majority of the IoT healthcare papers focus on information security issues. Healthcare is not highlighted as a major industry in [14][16]. This table illustrates that there is not even a single survey paper that focuses on how AI methods/techniques can be used to tackle security and privacy issues for various healthcare scenarios

III. Classification and Observations

This section analyzes and provides observations on the various IoT security issues in healthcare and how AI methods/techniques can be used in frameworks to resolve certain issues. For this purpose, we have collected related papers from the year 2014 to 2019 with experimental evaluation.

TABLE II. IoT Security in Healthcare

Paper Ref	Security Issues	Proposed Framework /Model	Experiment	Result

[17]	Physical protection for smart objects and maintenance of data confidentiality, integrity, and privacy.	Propose a secure IoT based HC system that operates through Body Sensor Network (BSN) architecture.	The scheme is tested on an IoT based testbed	The scheme can be implemented in mobile intelligent objects with strong security density.
[18]	Mutual authentication, confidentiality, anonymity, availability, forward security, and attack resistance	Review of ECC-based RFID authentication scheme based on performance and security	Computation and communication cost analysis with past ECC RFID schemes.	Three of the recently proposed schemes satisfy security requirements.
[19]	Data privacy, integrity. freshness, authentication, anonymity, and secure localization.	Secure IoT healthcare system using BSN care	Performance benchmarking based on security requirements and execution time.	The proposed system can satisfy the security requirements for the BSN healthcare system
[20]	Authentication and authorization	Session resumption-based end-to-end security scheme for IoT healthcare.	Security and performance evaluation	Proposed Scheme can provide end to end security for IoT healthcare
[21]	Privacy Breach of Healthcare data	Cloud-based healthcare service combined with IoHT for preserving the privacy of user's healthcare data.	Tested the performance, accuracy of the proposed framework.	Increase in privacy without affecting the accuracy of the framework.
[22]	Authentication of bio-information without compromising the owner's privacy.	Anonymous batch verification scheme for MHCS based on improved certificateless aggregate signature.	Performance evaluation based on computation overhead and storage overhead.	Achieves lower computation overhead and better efficiency.
[23]	Secure data transmission from sensors to doctors.	Robust and lightweight authentication scheme for WMSN.	Performance and simulation with NS3	The proposed scheme achieves high efficiency.
[24]	Securing healthcare data	GC architecture to secure the integration of fog and cloud computing.	Performance evaluation using sensitivity, specificity, precision, recall, and f-measure	The proposed architecture is efficient.
[25]	Reliable and secure data communication for IoT and Cloud infrastructure supported devices.	Neuro-Fuzzy Inference System with a brain-inspired trust management model	Simulation of proposed TMM in the NS-2 platform.	TMM was better than FIS based trust management algorithms in terms of accuracy.
[26]	Access to the server by attackers and entry of malicious devices	Device Authentication scheme which makes use of PUF for IoMT	Experimental evaluation and theoretical validation of PMSec	PUF can be used to authenticate devices in the network.
[27]	Security and privacy issues in healthcare data aggregation.	Privacy-preserving health data aggregation scheme for data collection	The proposed scheme is evaluated based on efficiency	Robust Security is achieved for health data aggregation.
[28]	Security and integrity of medical data	Hybrid Encryption Schema- a combination of advanced encryption standard, rivestm shamr, and adleman algorithms	Scheme is implemented using MATLAB software on a personal computer.	Scheme was able to protect patient data with high imperceptibility, minimal deterioration
[29]	Privacy and insecurity against attacks	Efficient pairing free aggregate signature scheme which can be used in certificateless system for HWMSNs.	Performance evaluation of the proposed CLAS scheme.	Proposed scheme has efficient aggregation and satisfies the security needs for HWMSNs.
[30]	Secure medical data transmission and resistance against various security attacks	Improving the security weakness of Liu-Chung's scheme using secure authentication and Data encryption for IoT medical care system.	Security analysis of the proposed scheme	Scheme shows that its ability to withstand attacks and satisfy security attributes.
[31]	Confidentiality of medical data	Instance of new and efficient SHE scheme for homomorphic evaluation based on existing SHE scheme	Performance evaluation of SIMD SHE FV, HDS, HCS, clustering and surf scheme for DR diagnosis.	Proposed scheme can perform classification on encrypted DR image
[32]	Access control, data confidentiality, and secure searching over ciphertext.	Lightweight keyword searchable encryption scheme along with fine-grained access control for health IoT Fog cloud framework.	Security and Efficiency analysis of the proposed scheme.	Scheme is secure and needs less storage, transmission, and computation cost.
[33]	Security and privacy of medical data	SAB-UAS scheme for secure communication of healthcare application	NS3 simulation using network parameters.	Proposed scheme is superior compared to other protocols.
[34]	Security and privacy of health data acquisition and transmission	Secure Data scheme for IoT based healthcare system	The scheme is analyzed based on FPGA simulation	Performance of the scheme is analyzed and validated via FPGA simulations
[35]	Privacy and confidentiality of patient profiles.	Fog-based middleware is hosted on the fog nodes for providing efficient aggregation	Performance evaluation based on the accuracy	Privacy is increased without affecting accuracy.

[36]	Security for the stored information	IoT based development framework for IoT cloud-centric communication	The framework is evaluated based on efficiency, security, adoption and predictive analysis of physical activities.	AES and RSA algorithms for thorough encryption and decryption for public and private clouds respectively.
[37]	Hardware attacks	Evaluation platform to evaluate software security in the early stages of the design phase.	Glitch&SCA, an evaluation platform to evaluate the design.	This platform shows the resilience of MCU without any countermeasures against the side-channel attacks.

TABLE III. AI SECURITY IN HEALTHCARE

Paper Ref	**Proposed framework/Model**	**AI Algorithm /Method**	**Security Services**	**Experiment Evaluation**	**Results**
[38]	eDiag, an online medical pre-diagnosis framework that is used for preserving the privacy of medical information	nonlinear support vector machine (SVM)	Preservation of confidential information about the prediction model of the healthcare provider.	Security analysis and performance evaluation of the proposed eDiag framework	eDiag can ensure confidentiality and privacy medical data and also has high efficiency
[39]	Pdiag, privacy-preserving diagnosis scheme based on naïve Bayes classification	Naive Bayes classifier	Privacy preservation of user's health information	PDiag performance evaluation based on accuracy and computational complexity.	Pdiag is efficient and shows its privacy and security abilities
[40]	HealthGuard, ML security framework for malicious detection in SHS (smart healthcare system)	ANN, DT RF and k-nearest neighbor	Detection of malicious activities in SHS	Performance evaluation against three malicious threats	HealthGuard security framework is effective for SHS with 91% accuracy.
[41]	Robust watermarking model for maintaining the robustness of embedded data using double-layer security	SVM classifier	Medical image security	Simulation to test the robustness and imperceptibility by measuring the PSNR and SSIM	Robustness and Imperceptibility- more than 0.5 for SSIM and more than 35 dB for PSNR
[42]	Tiger Hash sign based AdaBoost with SVM classifier to improve the security of multicasting routing in MANETs	SVM classifier	Secure multicast routing for mobile healthcare systems	Simulation of TH-ASVMC technique based on 4 metrics	TH-ASVMS can improve the reliability and rate of data integrity in multicast routing

TABLE IV. IOT SECURITY IN HEALTHCARE USING AI

Paper Ref	**Proposed Framework/Model**	**Security Issues**	**Challenges**	**AI method/Algorithm**	**Experimental Evaluation**	**Results**
[43]	MSCryptoNet to enable scalability and conversion of neural networks for preserving the privacy of the deep learning scheme.	Privacy of IoT in healthcare systems.	Application of multi-key homomorphic encryption, converting FHE scheme into multikey MK-FHE, privacy, and stability of the training model	Multi-Scheme Crypto Deep Neural Network	MSCryptoNet for privacy-preserving prediction and comparison of diabetes progression for patients using multiple datasets	MSCryptoNet shows no loss of accuracy and efficiency using dataset encrypted with different schemes or keys
[44]	A trust-based approach using Bayesian inference to find malicious devices in healthcare environment	Insider attacks	Threshold, Behavioral profile, large traffic volume, IT experts in HC area, security policy enforcement, implementation of additional security mechanisms	Bayesian Algorithm	Performance evaluation in simulated and real HC SDN environments	The proposed approach is feasible and effective in detecting malicious HC devices compared to another IDS mechanism.
[45]	Domain deep patient ECG image learning framework to overcome biometric user identification challenges	Security and privacy of smart health	Biometric user identification in ECG scenarios	Deep Convolutional Neural Network	Evaluation of the framework using two public databases.	Framework achieves 97.2% accuracy and is outperforms other existing frameworks
[46]	EDPDCS based on MapReduce framework to enable clustering analysis for privacy preservation	Personal information privacy	Trade-off between accuracy and privacy in privacy-preserving clustering algorithms.	k-means algorithm	Comparison of NICV clustering results of the proposed method with 2 datasets	The proposed framework can improve efficiency & accuracy of the clustering algorithm

[47]	Learning-based Deep Q n/w to manage health data and reduce malware attacks	Security, privacy and reliability of the healthcare system.	Privacy challenges and requirements in IoT Healthcare.	Deep Q Learning	NS2 simulation of framework security analysis is conducted and compared with other ML algorithms.	Framework achieves a minimum error rate and an increase in the malware detection rate

A. IoT Security in Healthcare

Table II is a study of related papers that discuss different kinds of security issues that are faced when using IoT in Healthcare. Some key observations are discussed in this section. (1) Healthcare data is susceptible to attacks which can lead to life-threatening consequences and its security is important. Most of the attacks discussed relate to the compromise of patient privacy. Authentication and authorization issues are also treated and approaches to resolving unauthorized access to patient profiles are proposed through numerous frameworks. (2) Only two papers propose frameworks related to the BSN architecture to secure IoT in healthcare. (3) From the proposed frameworks column, the majority of papers in Table II improve on existing schemes. (4) Cloud frameworks discussed in [21, 24 and 32], where preserving the privacy of the user's healthcare data from IoHT is treated. (5) Frameworks studied show that evaluation is performance benchmarked, with factors such as accuracy, security, and efficiency. (6) Simulation-based implementations and their numerical results are presented in 20% of the papers surveyed, [23 and 33], with NS3 being the most common platform used. (7) Testbed environments deployed for evaluation of proposed schemes and their experimental results are covered in 10% of the surveyed papers,[17]. (8) Of the papers which present experimental evaluation, a majority prove efficiency of the proposed scheme; a few papers demonstrate the extent to which security requirements are satisfied, while preserving privacy and accuracy.

B. AI Security in Healthcare

Table III presents a study of paper related to how AI security services can assist healthcare and further observations are discussed in this section. (9) The Frameworks proposed, provide security services using AI methods/techniques. (10) The proposed AI security services leans more towards preservation of patient privacy. (11) Among the AI methods/techniques used in the frameworks, SVM machine learning-based algorithm is the most commonly used algorithm to secure healthcare. (12) Simulation based experiments and numerical results are presented in [41 and 42]. (13) A majority of these papers do not provide a percentage of the effectiveness of their framework and more papers need to report it in the future.

C. IoT Security in Healthcare using AI

Table IV provides a study of how AI can be used for IoT security in Healthcare and further observations are discussed in this section. (14) A majority of the papers use deep neural networks for the security and privacy of healthcare systems. (15) A real healthcare SDN environment is used for performance evaluation in [44]. (16) Simulation based implementation and numerical results using NS-2 is presented in [47]. (17) All papers in this table undergo a comparison analysis that shows them outperforming other existing solutions.(18) None of the papers provide a comparison evaluation of different AI methods/techniques.

IV. Conclusion

This survey presents a study and analysis of different classifications based on past survey papers and journals papers between 2014 and 2019. A total of eighteen observations are discussed in this paper, taking into account both numerical and experimental evaluations presented in the surveyed papers with a focus on addressing security of IoT in healthcare. Security methods or techniques that employ AI based approaches for IoT in healthcare and associated frameworks are also surveyed. Our study showed that there is a lack of in-depth surveys published on the use of AI based approaches. Future work is highly recommended in this area.

References

[1] Almobaideen W, Krayshan R, Allan M and Saadeh M 2017 Internet of Things: Geographical Routing based on healthcare centers vicinity for mobile smart tourism destination *Technol. Forecast. Soc. Change* **123** 342–50

[2] Qasem M H and Almobaideen W 2019 Heterogeneity in IoT-Based Smart City Designs *Int. J. Interact. Mob. Technol.* **13** 210–25

[3] Khan S U, Islam N, Jan Z, Din I U, Khan A and Faheem Y 2019 An e-Health care services framework for the detection and classification of breast cancer in breast cytology images as an IoMT application *Futur. Gener. Comput. Syst.* **98** 286–96

[4] Al-Milli N and Almobaideen W 2019 Hybrid Neural Network to Impute Missing Data for IoT Applications *2019 IEEE Jordan Int. Jt. Conf. Electr. Eng. Inf. Technol. JEEIT 2019 - Proc.* 121–5

[5] Chhowa T T, Rahman M A, Paul A K and Ahmmed R 2019 A Narrative Analysis on Deep Learning in IoT based Medical Big Data Analysis with Future Perspectives *2nd Int. Conf. Electr. Comput. Commun. Eng. ECCE 2019* 1–6

[6] Ieracitano C, Adeel A, Gogate M, Dashtipour K, Morabito F C, Larijani H, Raza A and Hussain A 2018 Statistical Analysis Driven Optimized Deep Learning System for Intrusion Detection *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)* **10989 LNAI** 759–69

[7] Strielkina A, Illiashenko O, Zhydenko M and Uzun D 2018 Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment *Proc. 2018 IEEE 9th Int. Conf. Dependable Syst. Serv. Technol. DESSERT 2018* 67–73

[8] Al Alkeem E, Yeun C Y and Zemerly M J 2016 Security and privacy framework for ubiquitous healthcare IoT devices *2015 10th Int. Conf. Internet Technol. Secur. Trans. ICITST 2015* 70–5

[9] Saadeh M, Sleit A, Qatawneh M and Almobaideen W 2016 Authentication techniques for the internet of things: A survey *Proc. - 2016 Cybersecurity Cyberforensics Conf. CCC 2016* 28–34

[10] Jayalakshmi M and Gomathi V 2018 Pervasive health monitoring through video-based activity information integrated with sensor-cloud oriented context-aware decision support system *Multimed. Tools Appl.*

[11] Alharam A K and El-Madany W 2017 Complexity of cyber security architecture for IoT healthcare industry: A comparative study *Proc. - 2017 5th Int. Conf. Futur. Internet Things Cloud Work. W-FiCloud 2017* **2017-Janua** 246–50

[12] Saadeh M, Sleit A, Sabri K E and Almobaideen W 2018 Hierarchical architecture and protocol for mobile object authentication in the context of IoT smart cities *J. Netw. Comput. Appl.* **121** 1–19

[13] Williams P A H and McCauley V 2017 Always connected: The security challenges of the healthcare Internet of Things *2016 IEEE 3rd World Forum Internet Things, WF-IoT 2016* 30–5

[14] Al-garadi M A, Mohamed A, Al-ali A, Du X and Guizani M 2018 A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security *Polit. Q.* 42

[15] Ghosal P, Das D and Das I 2018 Extensive survey on cloud-based IoT-healthcare and security using machine learning *Proc. - 2018 4th IEEE Int. Conf. Res. Comput. Intell. Commun. Networks, ICRCICN 2018* 1–5

[16] Hussain F, Hussain R, Hassan S A and Hossain E 2019 Machine Learning in IoT Security: Current Solutions and Future Challenges

[17] Yeh K H 2016 A Secure IoT-Based Healthcare System with Body Sensor Networks *IEEE Access* **4** 10288–99

[18] He D and Zeadally S 2015 An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography *IEEE Internet Things J.* **2** 72–83

[19] Gope P and Hwang T 2016 BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network *IEEE Sens. J.* **16** 1368–76

[20] Moosavi S R, Gia T N, Nigussie E, Rahmani A M, Virtanen S, Tenhunen H and Isoaho J 2015 Session resumption-based end-to-end security for healthcare internet-of-things *Proc. - 15th IEEE Int. Conf. Comput. Inf. Technol. CIT 2015, 14th IEEE Int. Conf. Ubiquitous Comput. Commun. IUCC 2015, 13th IEEE Int. Conf. Dependable, Auton. Se* 581–8

[21] Elmisery A M, Rho S and Botvich D 2016 A fog based middleware for automated compliance with OECD privacy principles in internet of healthcare things *IEEE Access* **4** 8418–41

[22] Liu J, Cao H, Li Q, Cai F, Du X and Guizani M 2019 A large-scale concurrent data anonymous batch verification scheme for mobile healthcare crowd sensing *IEEE Internet Things J.* **6** 1321–30

[23] Wu F, Li X, Sangaiah A K, Xu L, Kumari S, Wu L and Shen J 2018 A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks *Futur. Gener. Comput. Syst.* **82** 727–37

[24] Manogaran G, Varatharajan R, Lopez D, Kumar P M, Sundarasekar R and Thota C 2018 A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system *Futur. Gener. Comput. Syst.* **82** 375–87

[25] Mahmud M, Kaiser M S, Rahman M M, Rahman M A, Shabut A, Al-Mamun S and Hussain A 2018 A Brain-Inspired Trust Management Model to Assure Security in a Cloud Based IoT Framework for Neuroscience Applications *Cognit. Comput.* **10** 864–73

[26] Yanambaka V P, Mohanty S P, Kougianos E and Puthal D 2019 PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things *IEEE Trans. Consum. Electron.* **65** 388–97

[27] Tang W, Ren J, Deng K and Zhang Y 2019 Secure Data Aggregation of Lightweight E-Healthcare IoT Devices with Fair Incentives *IEEE Internet Things J.* **6** 8714–26

[28] Elhoseny M, Ramírez-González G, Abu-Elnasr O M, Shawkat S A, Arunkumar N and Farouk A 2018 Secure Medical Data Transmission Model for IoT-Based Healthcare Systems *IEEE Access* **6** 20596–608

[29] Gayathri N B, Thumbur G, Rajesh Kumar P, Rahman M Z U, Reddy P V and Lay-Ekuakille A 2019 Efficient and Secure Pairing-Free Certificateless Aggregate Signature Scheme for Healthcare Wireless Medical Sensor Networks *IEEE Internet Things J.* **6** 9064–75

[30] Li C T, Wu T Y, Chen C L, Lee C C and Chen C M 2017 An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system *Sensors (Switzerland)* **17**

[31] Jiang L, Chen L, Giannetsos T, Luo B, Liang K and Han J 2019 Towards Practical Privacy-Preserving Processing over Encrypted Data in IoT: An Assistive Healthcare Use Case *IEEE Internet Things J.* **6** 1–1

[32] Li H and Jing T 2019 A lightweight fine-grained searchable encryption scheme in fog-based healthcare iot networks *Wirel. Commun. Mob. Comput.* **2019**

[33] Deebak B D, Al-Turjman F, Aloqaily M and Alfandi O 2019 An Authentic-Based Privacy Preservation Protocol for Smart e-Healthcare Systems in IoT *IEEE Access* **7** 135632–49

[34] Tao H, Bhuiyan M Z A, Abdalla A N, Hassan M M, Zain J M and Hayajneh T 2019 Secured Data Collection with Hardware-Based Ciphers for IoT-Based Healthcare *IEEE Internet Things J.* **6** 410–20

[35] Elmisery A M, Rho S and Aborizka M 2019 A new computing environment for collective privacy protection from constrained healthcare devices to IoT cloud services *Cluster Comput.* **22** 1611–38

[36] Gupta P K, Maharaj B T and Malekian R 2017 A novel and secure IoT based cloud centric architecture to perform predictive analysis of users activities in sustainable health centres *Multimed. Tools Appl.* **76** 18489–512

[37] Kazemi Z, Papadimitriou A, Hely D, Fazcli M and Beroulle V 2018 Hardware security evaluation platform for mcu-based connected devices: Application to healthcare IoT *2018 IEEE 3rd Int. Verif. Secur. Work. IVSW 2018* 87–92

[38] Zhu H, Liu X, Lu R and Li H 2017 Efficient and Privacy-Preserving Online Medical Prediagnosis Framework Using Nonlinear SVM *IEEE J. Biomed. Heal. Informatics* **21** 838–50

[39] Liu X, Zhu H, Lu R and Li H 2018 Efficient privacy-preserving online medical primary diagnosis scheme on naive bayesian classification *Peer-to-Peer Netw. Appl.* **11** 334–47

[40] Newaz A K M I, Sikder A K, Rahman M A and Uluagac A S 2019 HealthGuard : A Machine Learning-Based Security Framework for Smart Healthcare Systems *2019 Sixth Int. Conf. Soc. Networks Anal. Manag. Secur.* 389–96

[41] Rai A and Singh H V 2017 SVM based robust watermarking for enhanced medical image security *Multimed. Tools Appl.* **76** 18605–18

[42] Venkatesan R, Srinivasan B and Rajendiran P 2019 Tiger hash based AdaBoost machine learning classifier for secured multicasting in mobile healthcare system *Cluster Comput.* **22** 7039–53

[43] Kwabena O A, Qin Z, Qin Z and Zhuang T 2019 MSCryptoNet: Multi-Scheme Privacy-Preserving Deep Learning in Cloud Computing *IEEE Access* **7** 29344–54

[44] Meng W, Choo K K R, Furnell S, Vasilakos A V. and Probst C W 2018 Towards Bayesian-Based Trust Management for Insider Attacks in Healthcare Software-Defined Networks *IEEE Trans. Netw. Serv. Manag.* **15** 761–73

[45] Zhang Q 2019 Phase-domain Deep Patient-ECG Image Learning for Zero-effort Smart Health Security* *2019 41st Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.* 2622–8

[46] Guan Z, Lv Z, Du X, Wu L and Guizani M 2019 Achieving data utility-privacy tradeoff in Internet of Medical Things: A machine learning approach *Futur. Gener. Comput. Syst.* **98** 60–8

[47] Mohamed Shakeel P, Baskar S, Sarma Dhulipala V R, Mishra S and Jaber M M 2018 Maintaining Security and Privacy in Health Care System Using Learning Based Deep-Q-Networks *J. Med. Syst.* **42**