GSC Advanced Engineering and Technology

Cross Ref DOI: 10.30574/gscaet

Journal homepage: https://gsconlinepress.com/journals/gscaet/

(REVIEW ARTICLE)

A critical review of internet of things communication environment: Privacy and security constraints

Catherine Kanini *

Department of Computer Science, Kisii University, Kisii, Kenya.

GSC Advanced Engineering and Technology, 2022, 04(02), 042–057

Publication history: Received on 20 October 2022; revised on 01 December 2022; accepted on 03 December 2022

Article DOI: https://doi.org/10.30574/gscaet.2022.4.2.0047

Abstract

The recent past has experienced a steady increase in the adoption of Internet of Things (IoT) in a number of areas such as smart cities, smart homes, smart transportation and smart health. Due to the message exchanges among IoT devices over the public internet, the transmitted data is vulnerable to many security and privacy attacks. Therefore, many schemes have been presented over the recent past to address these challenges. However, many security holes still exist in most of the current techniques. It was also noted that the resource limited nature of most IoT devices renders traditional authentication schemes for main-powered systems with high processing power and large memory infeasible and inapplicable. To address this performance issue, numerous lightweight authentication schemes have been put forward. However, this paper discovered numerous security and privacy gaps in these schemes. Based on these shortcomings, recommendations are given towards the end of this paper which are very critical for security enhancements in this pervasive computing environment.

Keywords: IoT; Privacy; Security; Attacks; Ubiquity; Networks

1. Introduction

Ubiquitous computing is on the rise [1] owing to automation and intelligence brought about by the Internet of Things (IoT). Basically, IoT is a large network connecting smart devices together. These devices include sensors and actuators that have been adopted in a wide range of domains such as smart grids, public health, smart homes, waste management, smart cities, smart transportation, energy management and agriculture [2], [3], [4]. The goal of IoT is to enable heterogeneous devices to connect to the internet and exchange information in a reliable manner. In this environment, trillions of low power physical objects exchange messages with each other devoid of human intervention [5], [6]. In addition, IoT enables heterogeneous devices to be ubiquitously connected over the internet as well as enabling remote control of these devices [7] as shown in Figure 1. As explained in [8], IoT is the most significant technology in the healthcare sector.

Here, centralized health monitoring through IoT enhances efficiency, safety and convenience for the patients as well as the elderly [10]. The IoT devices are capable of collecting and analyzing data, as well as making autonomous decisions [11].

*Corresponding author: Catherine Kanini
Department of Computer Science, Kisii University, Kisii, Kenya

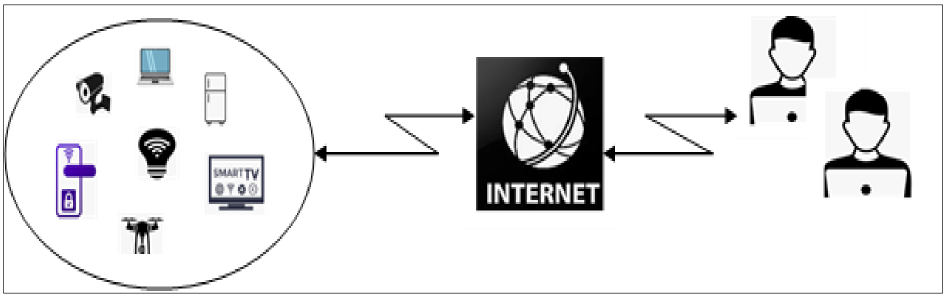

Figure 1 Communication in an IoT Environment

As shown in Figure 2, the IoT architecture comprises of four layers which include perception layer, network layer, middleware layer, and application layer [12]. The perception layer utilizes sensor nodes and other hardware to perceive and collects data [13]. On the other hand, the network layer facilitates connectivity among the devices as well as the internet. It also transmits and processes sensor data [14]. On its part, the middle layer sits in between the network and application layers. It serves to make intelligent decisions based on the processed results. In so doing, it efficiently delivers services while at the same time assuring interoperability and scalability [15], [16]. The application layer supports business services and analyzes the received information to facilitate intelligent decisions that meet user requirements [17]. These decisions may involve when to perform some activities in the network. This layer may comprise of diverse applications for the business needs, such as the Constrained Application Protocol (CoAP). This protocol is the hypertext transfer protocol (HTTP) replacement for resource-constrained devices [18], [19].

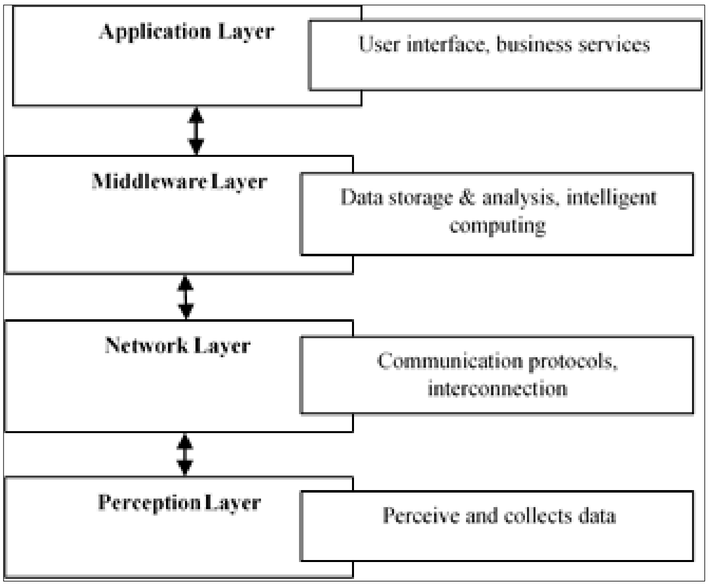

Figure 2 Basic IoT Layered Architecture

Although IoT devices offer convenience and increased efficiency, they introduce a number of threats and vulnerabilities that can be exploited by adversaries. The numerous attacks, threats and vulnerabilities can negatively affect the practical implementation of IoT networks [20], [21], [22], [23], [24]. As such, it is important to uphold integrity, confidentiality, authorization, confidentiality, privacy, availability and non-repudiation [25], [26], [27], [28], [29], [30]. In this communication environment, proper authentication serves as the first step towards perfect security [3], [31], [32], [33], [34]. This ensures that security threats such as packet replays and impersonations are kept at bay. This is particularly important now that IoT devices have been deployed in sensitive domains such as in the military and healthcare [35], [36], [37], [38], [39], [40].

According to [41] and [42], IoT networked devices have many security and privacy challenges. These include scalability, resources heterogeneity, lack of central control point and multiple attack surfaces. This is aggravated by the fact that conventional TCP/IP architecture deployed for network connectivity is not suitable for privacy and security enhancement in IoT [43]. As explained in [44], the frequent exchange of confidential data over IoT networks exposes them to various attacks such as fabrication, denial of service (DoS) and as eavesdropping.

Based on the foregoing discussion, the implementation of scalable, secure and private communication protocols in IoT is a challenging task. This can be partly due to the resource-limited nature of the IoT smart devices [45]. This limitation is reflected in their storage and computation efficiency. As such, the traditional security solutions are unsuitable for direct deployment in IoT networks [3]. This is due to their heavy computation loads [46] and large memory requirements. Therefore, as smart devices become increasingly connected, security, performance [47] and privacy issues need to be urgently looked into [7]. To this end, authentication, data encryption and authorization are some of the recommended practices towards the attainment of confidentiality [48], [49], [50], [51]. The contributions of this paper include the following:

- A thorough review of the legacy IoT security architecture is presented.
- A discussion of the strengths and weaknesses of the conventional IoT security techniques is provided.
- Towards the end of this paper, some recommendations are given which are thought to be essential during the design and development of perfect security solutions for the IoT environment.

The rest of this paper is structured as follows: Section 2 presents the related work, while Section 3 discusses the findings. In Section 4, some recommendations for improving IoT security posture are given. Finally, Section 5 concludes the paper and gives future research directions.

2. Related Work

Research on security and privacy issues in IoT has attracted a lot of attention and hence numerous schemes have been developed in literature. For instance, Physical Unclonable Functions (PUF) have been deployed to develop security solutions in [52], [53], [54], [55], [56], [57], [58] and [59]. However, PUF-based schemes have stability challenges [60]. To address this issue, improved authentication schemes are presented in [61] and [62]. However, the approach in [61] incurs high time complexity. To solve this issue, the lightweight scheme developed in [63] can be utilized. To authenticate the sensor node to the user, authors in [64] have introduced an Elliptic Curve Cryptography (ECC) and Key Distribution Centre (KDC) based scheme. However, KDC presents a single point of failure [65]. In addition, although a sensor node is authenticated, the user is not authenticated and hence this scheme cannot achieve perfect mutual authentication between user and sensor. To address this challenge, authors in [66] have presented a mutual authentication scheme in which the reader is equipped with cache for storage of tag secret keys. Although this scheme incurs minimal computation costs, this cache renders the reader susceptible to side-channeling attacks [67]. As such, an improved mutual authentication technique using a Challenge Handshake Authentication Protocol (CHAP) is developed in [68]. Identity-based schemes have also been deployed to offer security and privacy protection in IoT environment [69], [70], [71], [72], [73], [74], [75]. Unfortunately, identity-based schemes have key escrow issues [76]. Similarly, the identity-based aggregate signatures based scheme in [77], has key escrow challenges. This issue is solved by the sparse algorithm based technique in [78]. Similarly, the efficient key management mutual authentication protocol in [79] can address the issues with identity-based schemes.

Radio frequency identification (RFID) presents another important technology for securing IoT networks. For instance, RFID-based security techniques have been presented in [80], [81] and [82]. However, the security parameters are transmitted from the tag to the reader in plaintext [83]. In addition, RFID-based schemes are vulnerable to impersonation or cloning attacks [10]. To address this challenge, the protocol in [84] can be utilized. This is due to its security features such as un-traceability, user privacy, backward secrecy and strong forward secrecy. In addition, it is robust against node capture and impersonation attacks. Similarly, the protocol in [85] offers mutual authentication and is resilient against impersonation, packet replay, stolen verifier, DoS and password guessing attacks. Therefore, it can address the issues with RFID-based schemes. Authors in [86] have identified malicious manipulation of sensitive data, privacy breaches and unauthorized use of the data as serious issues in IoT. As such, they have introduced secure IoT-based cloud architecture. Similarly, the identification and authentication technique in [87] and digital signature based schemes in [88] and [89] can address security issues in IoT. Although the IoT health framework in [90] offers secure storage of shared health information, its design does not consider authentication or privacy.

The advanced encryption standard (AES) and the Rivest, Shamir and Adleman (RSA) algorithms have also been heavily utilized in IoT security. For instance, the authors in [91] have utilized RSA and AES to achieve the confidentiality, while authors in [92] and [93] have deployed AES for secure communication. On the other hand, authors in [94] have developed a two-way IoT authentication protocol using RSA based certificates. However, the usage of RSA and AES may be computationally intensive for resource constrained IoT devices [95]. As such, numerous lightweight authentication methods have been introduced in [96], [97], [98], [99], [100], [101] and [102]. To secure IoT healthcare communication process, an identification system is developed in [103] while a human recognition system is presented in [104].

Over the recent blockchain technology has gained popularity is privacy and security enhancement in IoT environment. For instance, blockchain based authentication methods have been introduced in [105] and [106]. However, blockchain technology has high storage and computation complexities [107]. Therefore, lightweight security techniques in [108] and [109] have been developed to address these shortcomings. To offer efficient key management, authors in [110] have presented one-time signature to be used for multicast authentication. Unfortunately, one-time signature based schemes have limitations regarding the size and the storage of the signature. This problem can potentially be addressed by the Chinese Remainder Theorem (CRT) based authentication method in [111] as well as the protocols in [112] and [113]. To securely authenticate resource-constrained devices, datagram transport layer security (DTLS) has been utilized in [114]. On the other hand, hyper elliptic curve based public key technique is developed in [115]. Similarly, a two-factor public key based authentication technique is presented in [116]. However, the public key infrastructure makes the scheme computationally extensive [117]. To address this problem, lightweight device authentication protocol in [118] and [119] can be utilized.

Based on Hash-based Message Authentication Code (HMAC), a privacy preserving scheme is developed in [120]. Similarly, a third party based privacy enhancement approach is presented in [121] while identity and service manager based authentication scheme is developed in [122]. However, the identity and service managers present single point of failure [123]. To address this challenge, asymmetric cryptography public key infrastructure based schemes have been introduced in [124], [125], [126] and [127]. However, the usage of PKI renders these methods computationally extensive [128]. As such, PKI digital certificates based protocol in [129] incurs high computation complexity. Therefore, the lightweight a new anonymous authentication method in [130] and lightweight biometric [131], and symmetric crypto-system in [132] can be utilized. On the other hand, authors in [133] have developed an inter-device authentication scheme that is demonstrated to be robust against man-in-the-middle and replay attacks [134].

To support secure and privacy-preserving communications, a group signature based scheme is developed in [135] and [136]. These protocols are shown to offer mutual authentication, anonymity, certificate revocation and traceability for malicious network entities. Similarly, group-based lightweight authentication methods have been presented in [137], [138] and [139]. However, these schemes can be compromised by malicious group members [140]. The protocol in [141] is shown to provide client privacy, attack resiliency, access control and data authentication. As such, it can address the issues with group-based authentication techniques. Although the method in [142] is robust against impersonation and replay attacks [143], it is susceptible to eavesdropping attacks [144]. This problem can be addressed by the scheme in [35] which offers authentication, access control, key management, secure routing and intrusion detection for secure IoT data transmission [145], [146]. To prevent replay attacks, a timestamp based authentication scheme is presented in [147]. However, the usage of timestamps renders this approach vulnerable to de-synchronization attacks [148]. Similarly, the scheme in [149] offers attacks resilience, privacy, network security, identity management and trust. However, this approach is unsuitable for resource-limited IoT devices due to high complexities. Therefore, an efficient smart card and password based authentication protocol presented in [150] can be utilized. Although this method offers mutual authentication and message confidentiality, it is susceptible to smart card loss attacks [151]. As such, the three-factor authentication approach in [152] has been presented to address this issue. To provide authorization in an IoT environment, security solutions are presented in [153] and [154]. Similarly, a decentralized privacy preserving authorization method is presented in [155].

It is evident from the above discussions that the assurance of security and privacy in IoT using the legacy methods is cumbersome. For instance, owing to the limitations of single-tier authentication architecture for IoT-cloud, authors in [156] have introduced a multi-tier authentication scheme based on usernames and passwords. However, low entropy passwords are vulnerable to brute-force attacks by polynomial time adversary [157]. A study in [158] pointed out that centralized authority architectures such as PKI is not appropriate for authentication and authorization in highly distributed IoT systems. This is because the central authority is overwhelmed with workloads in forms of large amounts of requests that cause significant delays [159]. To alleviate these issues, multi-layer security network models are presented in [160], [161], [162], [163] and [164] based on blockchains. Although these schemes protect user privacy, schemes based on blockchain technology have extensive computation and communication overheads [165]. In addition, lack of standard architecture and susceptibility to manipulation are other challenges of blockchain based security solutions [166]. Although the privacy and authentication protocol in [167] addresses some of these security issues, it has high slightly high execution time [168] which might not be ideal for IoT devices [169]-[180].

3. Results

The review above has shown that the IoT communication architecture consist of four layers, which include the perception, network, middleware and application. Table 1 presents the various security issues and attacks at each of these layers.

Table 1 IoT Layers Security Attacks and Issues

IoT Layer	Security Issues / Attacks	Security Goal Compromised
Perception layer	Denial of service attack, fake node or malicious data, jamming, tampering, node capture	Integrity, authentication, confidentiality, availability
Network layer	Cluster security problems, DoS and DDOS attacks, spoofed, altered or replayed routing information, man-in-the-middle attack, malicious code injection,	Authentication, integrity, availability
Middleware layer	Making intelligent decision processing huge data, malicious-code attacks, multi-party authentication, handling suspicious information, securely storing data in the cloud	Integrity, confidentiality
Application layer	Software vulnerabilities, spear-phishing attack, malicious code attacks, inability to receive security patches, hacking into the smart meter/grid,	Data privacy, access control

The various security and privacy goals that are compromised by the attacks and security vulnerabilities are also presented. It is evident that all the four IoT layers have numerous security vulnerabilities that can be exploited by adversaries to compromise the network. As such, a number of security solutions have been presented in literature. Table 2 gives a summary of these schemes.

Table 2 IoT Security Schemes

Scheme	Challenges
Mukhopadhyay, [52]	Stability challenges
Srinivasu et al. [53]	
Zhao et al. [54]	
Wallrabenstein, [55]	
Aman et al. [56]	
Xu et al. [57]	
Gope et al. [58]	
Huth et al. [59]	
El Zouka et al. [61]	High time complexity
Wang et al. [64]	KDC presents a single point of failure; user is not authenticated
Fan et al. [66]	Susceptible to side-channeling attacks
Salman et al. [69]	Have key escrow issues
Kim et al. [70]	
Wazid et al. [71]	
Al-Mahmud et al. [72]	
Gope et al. [73]	
Aman et al. [74]	
Zhao et al. [75]	
Zhang et al. [77]	

Aggarwal et al. [80]	Security parameters are transmitted from the tag to the reader in plaintext; vulnerable to impersonation or cloning attacks
Lee et al. [81]	
Yang et al. [82]	
Tyagi et al. [90]	Its design does not consider authentication or privacy
Mahmood et al. [91]	Computationally intensive
Jan et al. [92]	
Moghaddam et al. [93]	
Kothmayr et al. [94]	
Hammi et al. [105]	High storage and computation complexities
Ratheeet al. [106]	
Rashid et al. [160]	
Panarello et al. [161]	
Dorri et al. [162]	
Pinno et al. [163]	
[Rahulamathavan et al., 2017]	
Ji et al. [110]	Limitations regarding the size and the storage of the signature
Alizai et al. [116]	Computationally extensive
Horrow et al. [122]	Single point of failure
Tangade et al. [124]	Computationally extensive
Dolev et al. [125]	
Pranata et al. [126]	
Hong et al. [127]	
Karthikeyan et al. [129]	
Shao et al. [135]	Can be compromised by malicious group members
Shao et al. [136]	
Lai et al. [137]	
Fu et al. [138]	
Lai et al. [139]	
Emerson et al. [142]	Susceptible to eavesdropping attacks
Muhal et al. [147]	Vulnerable to de-synchronization attacks
Vasilomanolakis et al. [149]	High complexities
Kumar et al. [150]	Susceptible to smart card loss attacks
Singh et al. [156]	Vulnerable to brute-force attacks
Ukil et al. [167]	Slightly high execution time

Based on the information presented in Table 2, majority of the security schemes that have been developed so far for the IoT communication scenario still have numerous privacy, performance and security challenges. There is therefore need for improved security solutions that will effectively address the identified security gaps. As such, the recommendations in Section 4 below are deemed necessary during the design of IoT authentication schemes.

Recommendations

The literature reviewed has shown that the legacy IoT security solutions have numerous privacy, performance and security challenges. Therefore, the following recommendations are thought to be essential for the efficient preservation of security and privacy.

- It has been shown that most of the IoT devices are resource limited in terms of processing power, battery, and memory and communication capabilities. Therefore, the security solutions in this environment should be lightweight so as not to put much strain on these devices.
- IoT application domains include in the military and healthcare. As such, all the security protocols should be extensively analyzed and evaluated against conventional attack vectors such as node capture, Sybil, man-in-the-middle, denial of service, password guessing, packet replays, forgery, collision, brute force, dictionary and chosen-plaintext.
- Any secure communication protocol must take identity and location privacy into consideration.
- During mutual authentication, the number of messages exchanged among the communicating entities should be kept at minimum. This is to ensure that the communication costs are minimized. In addition, the sizes of the exchanged messages should be as small as possible due to the restricted bandwidth of the deployed communication protocols.
- When designing security protocols, lightweight cryptographic algorithms should be considered. This goes a long way in ensuring that the computation overheads are as low as possible.
- All authentication schemes should be scalable such that it is easy to add new nodes devoid of further setup or configuration. High scalability will also ensure that the authentication schemes are able to manage a large number of IoT devices.
- The design of an effective authentication service should be ensured for all the IoT architecture layers: the application, middleware, network and perception.
- The IoT communication devices are heterogeneous in nature. As such, IoT authentication schemes must take this heterogeneity into consideration during the design phase.
- In most cases, physical security of IoT devices is ignored since hardware security tends to be more expensive than software security. Therefore, there is need to incorporate hardware security with software security. This hardware security can be attained using PUF.
- Security aspects such as authentication, key management, access control and authorization should be energy aware.
- IoT communication environment yields massive heterogeneous data within a very short duration. Therefore, future focus should be the incorporation of technologies such as big data, fog computing, cloud computing and blockchain for the massive data exchange in IoT networks.

Given the prevalence of intrusions in IoT environment, there is need to combine formal techniques with machine learning for security vulnerabilities detection. These formal methods are vital in the provision of rigorous mathematical and logical guarantees for the safety and security properties of IoT security protocols.

4. Conclusion

IoT networks have continued to be deployed in numerous fields such as in smart homes, smart cities, smart agriculture, military, fire monitoring and smart healthcare. In some of these application domains, massive private and sensitive data items are being exchanged among the communicating entities. There is therefore need to protect the security and privacy of these massive data items. To this end, numerous security solutions have been developed in literature. This paper sought to provide an extensive review of these security schemes. Based on the findings, a plethora of security protocols have been presented, but which have a number of security vulnerabilities. The successful exploitation of these security holes can have devastating effects such as overdosing patients in smart healthcare due to message replays. Towards the end of this paper, recommendations have been given which are critical for perfect security in IoT application domains. Future work lies in the practical implementations of these recommendations so that necessary analysis and evaluation can be executed.

Compliance with ethical standards

Acknowledgments

I would like to thank my colleagues for the inspiration and assistance offered during the development and revision of this article.

References

[1] Khan MA, Quasim MT, Alghamdi NS, Khan MY. A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data. IEEE Access. 2020 Mar 13; 8:52018-27.

[2] Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Khalefa MS, Honi DG. MAC-Based Symmetric Key Protocol for Secure Traffic Forwarding in Drones. InInternational Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures 2022 (pp. 16-36). Springer, Cham.

[3] Mehta M, Patel K. A review for IOT authentication–current research trends and open challenges. Materials Today: Proceedings. 2020 Dec 9: 1-7.

[4] Choi SK, Ko JS, Kwak J. A study on IoT device authentication protocol for high speed and lightweight. In 2019 International Conference on Platform Technology and Service (PlatCon) 2019 Jan 28 (pp. 1-5). IEEE.

[5] Surendran S, Nassef A, Beheshti BD. A survey of cryptographic algorithms for IoT devices. In 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT) 2018 May 4 (pp. 1-8). IEEE.

[6] Nyangaresi VO, Ogundoyin SO. Certificate Based Authentication Scheme for Smart Homes. In 2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 202-207). IEEE.

[7] Deep S, Zheng X, Jolfaei A, Yu D, Ostovari P, Kashif Bashir A. A survey of security and privacy issues in the Internet of Things from the layered context. Transactions on Emerging Telecommunications Technologies. 2022 Jun; 33(6):e3935.

[8] Khoi NM, Saguna S, Mitra K, Åhlund C. IReHMo: An efficient IoT-based remote health monitoring system for smart regions. In 2015 17th International Conference on E-health Networking, Application & Services (HealthCom) 2015 Oct 14 (pp. 563-568). IEEE.

[9] Abood EW, Hussien ZA, Kawi HA, Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Kalafy SA. Provably secure and efficient audio compression based on compressive sensing. International Journal of Electrical and Computer Engineering (IJECE). 2023 Feb;13(1):335-46.

[10] El-Hajj M, Fadlallah A, Chamoun M, Serhrouchni A. A survey of internet of things (IoT) authentication schemes. Sensors. 2019 Mar 6; 19(5):1141.

[11] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In 2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[12] Adat V, Gupta BB. Security in Internet of Things: issues, challenges, taxonomy, and architecture. Telecommunication Systems. 2018 Mar; 67(3):423-41.

[13] Puthal D, Nepal S, Ranjan R, Chen J. Threats to networking cloud and edge datacenters in the Internet of Things. IEEE Cloud Computing. 2016 Jul 4; 3(3):64-71.

[14] Bello O, Zeadally S, Badra M. Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT). Ad Hoc Networks. 2017 Mar 15; 57:52-62.

[15] da Cruz MA, Rodrigues JJ, Al-Muhtadi J, Korotaev VV, de Albuquerque VH. A reference model for internet of things middleware. IEEE Internet of Things Journal. 2018 Jan 23;5(2):871-83.

[16] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Sep; 3(5):1-16.

[17] Jing Q, Vasilakos AV, Wan J, Lu J, Qiu D. Security of the Internet of Things: perspectives and challenges. Wireless Networks. 2014 Nov; 20(8):2481-501.

[18] Saadeh M, Sleit A, Qatawneh M, Almobaideen W. Authentication techniques for the internet of things: A survey. In 2016 cybersecurity and cyberforensics conference (CCC) 2016 Aug 2 (pp. 28-34). IEEE.

[19] Al Sibahee MA, Abdulsada AI, Abduljabbar ZA, Ma J, Nyangaresi VO, Umran SM. Lightweight, Secure, Similar-Document Retrieval over Encrypted Data. Applied Sciences. 2021 Dec 17; 11(24):12040.

[20] Yu D, Jin Y, Zhang Y, Zheng X. A survey on security issues in services communication of Microservices-enabled fog applications. Concurrency and Computation: Practice and Experience. 2019 Nov 25; 31(22):e4436.

[21] Pan L, Zheng X, Chen HX, Luan T, Bootwala H, Batten L. Cyber security attacks to modern vehicular systems. Journal of information security and applications. 2017 Oct 1; 36:90-100.

[22] Zheng X, Pan L, Yilmaz E. Security analysis of modern mission critical android mobile applications. In Proceedings of the Australasian Computer Science Week Multiconference 2017 Jan 31 (pp. 1-9).

[23] Radhappa H, Pan L, Xi Zheng J, Wen S. Practical overview of security issues in wireless sensor network applications. International journal of computers and applications. 2018 Oct 2; 40(4):202-13.

[24] Nyangaresi VO. ECC based authentication scheme for smart homes. In 2021 International Symposium ELMAR 2021 Sep 13 (pp. 5-10). IEEE.

[25] Zheng X, Pan L, Chen H, Di Pietro R, Batten L. A testbed for security analysis of modern vehicle systems. In 2017 IEEE Trustcom/BigDataSE/ICESS 2017 Aug 1 (pp. 1090-1095). IEEE.

[26] Nyangaresi VO, Abduljabbar ZA, Al Sibahee MA, Ibrahim A, Yahya AN, Abduljaleel IQ, Abood EW. Optimized Hysteresis Region Authenticated Handover for 5G HetNets. InArtificial Intelligence and Sustainable Computing 2022 (pp. 91-111). Springer, Singapore.

[27] Husamuddin M, Qayyum M. Internet of Things: A study on security and privacy threats. In 2017 2nd International Conference on Anti-Cyber Crimes (ICACC) 2017 Mar 26 (pp. 93-97). IEEE.

[28] Hussain MA, Hussien ZA, Abduljabbar ZA, Ma J, Al Sibahee MA, Hussain SA, Nyangaresi VO, Jiao X. Provably throttling SQLI using an enciphering query and secure matching. Egyptian Informatics Journal. 2022 Nov 16: 1-18.

[29] Mahmoud R, Yousuf T, Aloul F, Zualkernan I. Internet of things (IoT) security: Current status, challenges and prospective measures. In 2015 10th international conference for internet technology and secured transactions (ICITST) 2015 Dec 14 (pp. 336-341). IEEE.

[30] Nyangaresi VO. Provably Secure Protocol for 5G HetNets. In 2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2021 Nov 1 (pp. 17-22). IEEE.

[31] Nandy T, Idris MY, Noor RM, Kiah LM, Lun LS, Juma'at NB, Ahmedy I, Ghani NA, Bhattacharyya S. Review on security of Internet of Things authentication mechanism. IEEE Access. 2019 Oct 16; 7:151054-89.

[32] Hassan WH. Current research on Internet of Things (IoT) security: A survey. Computer networks. 2019 Jan 15; 148:283-94.

[33] Abduljabbar ZA, OmolloNyangaresi V, Al Sibahee MA, Ghrabat MJ, Ma J, QaysAbduljaleel I, Aldarwish AJ. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks. 2022 Sep 19;11(3):55.

[34] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Jun 25:100210.

[35] Zhao K, Ge L. A survey on the internet of things security. In 2013 Ninth international conference on computational intelligence and security 2013 Dec 14 (pp. 663-667). IEEE.

[36] Zhang C, Wu X, Zheng X, Yu S. Driver drowsiness detection using multi-channel second order blind identifications. IEEE Access. 2019 Jan 10; 7:11829-43.

[37] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. InEAI International Conference on Applied Cryptography in Computer and Communications 2022 (pp. 46-64). Springer, Cham.

[38] Abkenar AB, Loke SW, Zheng JX, Zaslavsky A. Service-mediated on-road situation-awareness for group activity safety. In Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services 2017 Nov 7 (pp. 478-481).

[39] Lu J, Wang J, Zheng X, Karmakar C, Rajasegarar S. Detection of smoking events from confounding activities of daily living. In Proceedings of the Australasian Computer Science Week Multiconference 2019 Jan 29 (pp. 1-9).

[40] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In 2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[41] Dorri A, Kanhere SS, Jurdak R. Blockchain in internet of things: challenges and solutions. arXiv preprint arXiv:1608.05187. 2016 Aug 18.

[42] Zhang ZK, Cho MC, Wang CW, Hsu CW, Chen CK, Shieh S. IoT security: ongoing challenges and research opportunities. In2014 IEEE 7th international conference on service-oriented computing and applications 2014 Nov 17 (pp. 230-234). IEEE.

[43] Khan R, Khan SU, Zaheer R, Khan S. Future internet: the internet of things architecture, possible applications and key challenges. In2012 10th international conference on frontiers of information technology 2012 Dec 17 (pp. 257-260). IEEE.

[44] Bhardwaj I, Kumar A, Bansal M. A review on lightweight cryptography algorithms for data security and authentication in IoTs. In 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC) 2017 Sep 21 (pp. 504-509). IEEE.

[45] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. In International Conference on Internet of Things as a Service 2022 (pp. 3-18). Springer, Cham.

[46] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably Secure and Fast Color Image Encryption Algorithm Based on S-Boxes and Hyperchaotic Map. IEEE Access. 2022 Feb 11;10:26257-70.

[47] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV Computing-Assisted Search and Rescue Mission Framework for Disaster and Harsh Environment Mitigation. Drones. 2022 Jun 22;6(7):154.

[48] Miorandi D, Sicari S, De Pellegrini F, Chlamtac I. Internet of things: Vision, applications and research challenges. Ad hoc networks. 2012 Sep 1; 10(7):1497-516.

[49] Abduljaleel IQ, Abduljabbar ZA, Al Sibahee MA, Ghrabat MJ, Ma J, Nyangaresi VO. A Lightweight Hybrid Scheme for Hiding Text Messages in Colour Images Using LSB, Lah Transform and Chaotic Techniques. Journal of Sensor and Actuator Networks. 2022 Oct 17;11(4):66.

[50] Bhabad MA, Bagade ST. Internet of things: architecture, security issues and countermeasures. International Journal of Computer Applications. 2015 Jan 1;125(14).

[51] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. InInternational Conference for Emerging Technologies in Computing 2021 Aug 18 (pp. 3-20). Springer, Cham.

[52] Mukhopadhyay D. PUFs as promising tools for security in internet of things. IEEE Design & Test. 2016 Apr 1; 33(3):103-15.

[53] Srinivasu B, Vikramkumar P, Chattopadhyay A, Lam KY. CoLPUF: a novel configurable LFSR-based PUF. In 2018 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS) 2018 Oct 26 (pp. 358-361). IEEE.

[54] Zhao M, Yao X, Liu H, Ning H. Physical unclonable function based authentication protocol for unit IoT and ubiquitous IoT. In 2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI) 2016 Oct 20 (pp. 179-184). IEEE.

[55] Wallrabenstein JR. Practical and secure IoT device authentication using physical unclonable functions. In2016 IEEE 4th international conference on future internet of things and cloud (FiCloud) 2016 Aug 22 (pp. 99-106). IEEE.

[56] Aman MN, Chua KC, Sikdar B. Mutual authentication in IoT systems using physical unclonable functions. IEEE Internet of Things Journal. 2017 May 10; 4(5):1327-40.

[57] Xu H, Ding J, Li P, Zhu F, Wang R. A lightweight RFID mutual authentication protocol based on physical unclonable function. Sensors. 2018 Mar 2; 18(3):760.

[58] Gope P, Lee J, Quek TQ. Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions. IEEE Transactions on Information Forensics and Security. 2018 May 3; 13(11):2831-43.

[59] Huth C, Zibuschka J, Duplys P, Güneysu T. Securing systems on the Internet of Things via physical properties of devices and communications. In 2015 Annual IEEE Systems Conference (SysCon) Proceedings 2015 Apr 13 (pp. 8-13). IEEE.

[60] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[61] El Zouka HA, Hosni MM. Secure IoT communications for smart healthcare monitoring system. Internet of Things. 2021 Mar 1;13:100036.

[62] Altan G, Kutlu Y, Yeniad M. ECG based human identification using Second Order Difference Plots. Computer Methods and programs in Biomedicine. 2019 Mar 1; 170:81-93.

[63] Li H, Lu R, Zhou L, Yang B, Shen X. An efficient merkle-tree-based authentication scheme for smart grid. IEEE Systems Journal. 2013 Jul 18; 8(2):655-63.

[64] Wang H, Sheng B, Li Q. Elliptic curve cryptography-based access control in sensor networks. International Journal of Security and Networks. 2006 Jan 1;1(3-4):127-37..

[65] Nyangaresi VO, Moundounga AR. Secure Data Exchange Scheme for Smart Grids. In 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[66] Fan K, Gong Y, Liang C, Li H, Yang Y. Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G. Security and Communication Networks. 2016 Nov 10;9(16):3095-104.

[67] Nyangaresi VO. Lightweight Anonymous Authentication Protocol for Resource-Constrained Smart Home Devices Based on Elliptic Curve Cryptography. Journal of Systems Architecture. 2022 Oct 18:102763.

[68] Roberts B, Akkaya K, Bulut E, Kisacikoglu M. An authentication framework for electric vehicle-to-electric vehicle charging applications. In2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS) 2017 Oct 22 (pp. 565-569). IEEE.

[69] Salman O, Abdallah S, Elhajj IH, Chehab A, Kayssi A. Identity-based authentication scheme for the Internet of Things. In2016 IEEE Symposium on Computers and Communication (ISCC) 2016 Jun 27 (pp. 1109-1111). IEEE.

[70] Kim H, Lee EA. Authentication and Authorization for the Internet of Things. IT Professional. 2017 Oct 4;19(5):27-33.

[71] Wazid M, Das AK, Odelu V, Kumar N, Conti M, Jo M. Design of secure user authenticated key management protocol for generic IoT networks. IEEE Internet of Things Journal. 2017 Dec 6;5(1):269-82.

[72] Al-Mahmud A, Morogan MC. Identity-based authentication and access control in wireless sensor networks. International Journal of Computer Applications. 2012 Jan 1;41(13).

[73] Gope P, Sikdar B. Lightweight and privacy-preserving two-factor authentication scheme for IoT devices. IEEE Internet of Things Journal. 2018 Jun 12; 6(1):580-9.

[74] Aman MN, Basheer MH, Sikdar B. Two-factor authentication for IoT with location information. IEEE Internet of Things Journal. 2018 Nov 21; 6(2):3335-51.

[75] Zhao Y, Li S, Jiang L. Secure and efficient user authentication scheme based on password and smart card for multiserver environment. Security and Communication Networks. 2018 Apr; 2018: 1-13.

[76] Nyangaresi VO, Morsy MA. Towards Privacy Preservation in Internet of Drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[77] Zhang L, Hu C, Wu Q, Domingo-Ferrer J, Qin B. Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response. IEEE Transactions on Computers. 2015 Oct 1; 65(8):2562-74.

[78] Goshvarpour A, Goshvarpour A. Human identification using a new matching pursuit-based feature set of ECG. Computer methods and programs in biomedicine. 2019 Apr 1;172:87-94.

[79] Nicanfar H, Jokar P, Beznosov K, Leung VC. Efficient authentication and key management mechanisms for smart grid communications. IEEE systems journal. 2013 Jul 4;8(2):629-40.

[80] Aggarwal R, Das ML. RFID security in the context of" internet of things". InProceedings of the First International Conference on Security of Internet of Things 2012 Aug 17 (pp. 51-56). ACM.

[81] Lee JY, Lin WC, Huang YH. A lightweight authentication protocol for internet of things. In2014 International Symposium on Next-Generation Electronics (ISNE) 2014 May 7 (pp. 1-2). IEEE.

[82] Yang K, Forte D, Tehranipoor MM. Protecting endpoint devices in IoT supply chain. In2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD) 2015 Nov 2 (pp. 351-356). IEEE.

[83] Nyangaresi VO, Abduljabbar ZA, Ma J, Al Sibahee MA. Verifiable Security and Privacy Provisioning Protocol for High Reliability in Smart Healthcare Communication Environment. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 569-574). IEEE.

[84] Gope P, Hwang T. A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks. IEEE Transactions on industrial electronics. 2016 Jun 27; 63(11):7124-32.

[85] Qi M, Chen J, Chen Y. A secure authentication with key agreement scheme using ECC for satellite communication systems. International Journal of Satellite Communications and Networking. 2019 May; 37(3):234-44.

[86] Gupta PK, Maharaj BT, Malekian R. A novel and secure IoT based cloud centric architecture to perform predictive analysis of users activities in sustainable health centres. Multimedia Tools and Applications. 2017 Sep; 76(18):18489-512.

[87] Pinto JR, Cardoso JS, Lourenço A, Carreiras C. Towards a continuous biometric system based on ECG signals acquired on the steering wheel. Sensors. 2017 Sep 28; 17(10):2228.

[88] Li D, Aung Z, Williams JR, Sanchez A. Efficient authentication scheme for data aggregation in smart grid with fault tolerance and fault diagnosis. In 2012 IEEE PES Innovative Smart Grid Technologies (ISGT) 2012 Jan 16 (pp. 1-8). IEEE.

[89] Nyangaresi VO, Abduljabbar ZA, Abduljabbar ZA. Authentication and Key Agreement Protocol for Secure Traffic Signaling in 5G Networks. In 2021 IEEE 2nd International Conference on Signal, Control and Communication (SCC) 2021 Dec 20 (pp. 188-193). IEEE.

[90] Tyagi S, Agarwal A, Maheshwari P. A conceptual framework for IoT-based healthcare system using cloud computing. In 2016 6th International Conference-Cloud System and Big Data Engineering (Confluence) 2016 Jan 14 (pp. 503-507). IEEE.

[91] Mahmood K, Chaudhry SA, Naqvi H, Shon T, Ahmad HF. A lightweight message authentication scheme for smart grid communications in power sector. Computers & Electrical Engineering. 2016 May 1; 52:114-24.

[92] Jan MA, Khan F, Alam M, Usman M. A payload-based mutual authentication scheme for Internet of Things. Future Generation Computer Systems. 2019 Mar 1; 92:1028-39.

[93] Moghaddam FF, Moghaddam SG, Rouzbeh S, Araghi SK, Alibeigi NM, Varnosfaderani SD. A scalable and efficient user authentication scheme for cloud computing environments. In2014 IEEE Region 10 Symposium 2014 Apr 14 (pp. 508-513). IEEE.

[94] Kothmayr T, Schmitt C, Hu W, Brünig M, Carle G. DTLS based security and two-way authentication for the Internet of Things. Ad Hoc Networks. 2013 Nov 1;11(8):2710-23.

[95] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[96] Ye N, Zhu Y, Wang RC, Malekian R, Lin QM. An efficient authentication and access control scheme for perception layer of internet of things. 2014 April; 8: 1617–1624.

[97] Fan K, Song P, Yang Y. ULMAP: Ultralightweight NFC mutual authentication protocol with pseudonyms in the tag for IoT in 5G. Mobile Information Systems. 2017 Apr 27;2017:1-7.

[98] Nyangaresi VO, Ma J, Al Sibahee MA, Abduljabbar ZA. Packet Replays Prevention Protocol for Secure B5G Networks. InProceedings of Seventh International Congress on Information and Communication Technology 2023 (pp. 507-522). Springer, Singapore.

[99] Al Salami S, Baek J, Salah K, Damiani E. Lightweight encryption for smart home. In 2016 11th International conference on availability, reliability and security (ARES) 2016 Aug 31 (pp. 382-388). IEEE.

[100] Porambage P, Schmitt C, Kumar P, Gurtov A, Ylianttila M. PAuthKey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications. International Journal of Distributed Sensor Networks. 2014 Jul 10; 10(7):357430.

[101] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In 2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[102] Fouda MM, Fadlullah ZM, Kato N, Lu R, Shen X. Towards a light-weight message authentication mechanism tailored for smart grid communications. In 2011 IEEE conference on computer communications workshops (INFOCOM WKSHPS) 2011 Apr 10 (pp. 1018-1023). IEEE.

[103] Alotaiby TN, Alshebeili SA, Aljafar LM, Alsabhan WM. ECG-based subject identification using common spatial pattern and SVM. Journal of Sensors. 2019 Mar 31;2019:1-9

[104] El_Rahman SA. Biometric human recognition system based on ECG. Multimedia Tools and Applications. 2019 Jul;78(13):17555-72.

[105] Hammi MT, Hammi B, Bellot P, Serhrouchni A. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. Computers & Security. 2018 Sep 1; 78:126-42.

[106] Rathee G, Sharma A, Saini H, Kumar R, Iqbal R. A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. Multimedia Tools and Applications. 2020 Apr; 79(15):9711-33.

[107] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[108] Hammi MT, Livolant E, Bellot P, Serhrouchni A, Minet P. A lightweight mutual authentication protocol for the IoT. InInternational Conference on Mobile and Wireless Technology 2017 Jun 26 (pp. 3-12). Springer, Singapore.

[109] Zhou L, Li X, Yeh KH, Su C, Chiu W. Lightweight IoT-based authentication scheme in cloud computing circumstance. Future Generation Computer Systems. 2019 Feb 1;91:244-51.

[110] Ji C, Kim J, Lee JY, Hong M. Review of one-time signatures for multicast authentication in smart grid. In2015 12th International Conference & Expo on Emerging Technologies for a Smarter World (CEWIT) 2015 Oct 19 (pp. 1-4). IEEE.

[111] Wen M, Lei J, Li J, Wang Y, Chen K. Efficient user access control mechanism for wireless multimedia sensor networks. Journal of Computational Information Systems. 2011; 7(9):3325-32.

[112] Nyangaresi VO, Abd-Elnaby M, Eid MM, NabihZakiRashed A. Trusted authority based session key agreement and authentication algorithm for smart grid networks. Transactions on Emerging Telecommunications Technologies. 2022 May 6:e4528.

[113] Nicanfar H, Jokar P, Leung VC. Smart grid authentication and key management for unicast and multicast communications. In2011 IEEE PES Innovative Smart Grid Technologies 2011 Nov 13 (pp. 1-8). IEEE.

[114] Dos Santos GL, Guimarães VT, da Cunha Rodrigues G, Granville LZ, Tarouco LM. A DTLS-based security architecture for the Internet of Things. In 2015 IEEE symposium on computers and communication (ISCC) 2015 Jul 6 (pp. 809-815). IEEE.

[115] Kavitha S, Alphonse PJ, Reddy YV. An improved authentication and security on efficient generalized group key agreement using hyper elliptic curve based public key cryptography for IoT health care system. Journal of medical systems. 2019 Aug; 43(8):1-6.

[116] Alizai ZA, Tareen NF, Jadoon I. Improved IoT device authentication scheme using device capability and digital signatures. In 2018 International Conference on Applied and Engineering Mathematics (ICAEM) 2018 Sep 4 (pp. 1-5). IEEE.

[117] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. In The Fifth International Conference on Safety and Security with IoT 2023 (pp. 81-99). Springer, Cham.

[118] Chen D, Zhang N, Qin Z, Mao X, Qin Z, Shen X, Li XY. S2M: A lightweight acoustic fingerprints-based wireless device authentication protocol. IEEE Internet of Things Journal. 2016 Oct 20;4(1):88-100.

[119] Zhang C, Green R. Communication security in internet of thing: preventive measure and avoid DDoS attack over IoT network. InProceedings of the 18th symposium on communications & networking 2015 Apr 12 (pp. 8-15).

[120] Chim TW, Yiu SM, Hui LC, Li VO. PASS: Privacy-preserving authentication scheme for smart grid network. In2011 IEEE International Conference on Smart Grid Communications (SmartGridComm) 2011 Oct 17 (pp. 196-201). IEEE.

[121] Tao H, Peiran W. Preference-based privacy protection mechanism for the internet of things. In 2010 Third International Symposium on Information Science and Engineering 2010 Dec 24 (pp. 531-534). IEEE.

[122] Horrow S, Sardana A. Identity management framework for cloud based internet of things. In Proceedings of the First International Conference on Security of Internet of Things 2012 Aug 17 (pp. 200-203). ACM.

[123] Nyangaresi VO. A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. In the 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation. 2021 Nov; 605-612.

[124] Tangade S, Manvi SS. Scalable and privacy-preserving authentication protocol for secure vehicular communications. In 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) 2016 Nov 6 (pp. 1-6). IEEE.

[125] Dolev S, Krzywiecki Ł, Panwar N, Segal M. Vehicle authentication via monolithically certified public key and attributes. Wireless Networks. 2016 Apr; 22(3):879-96.

[126] Pranata H, Athauda R, Skinner G. Securing and governing access in ad-hoc networks of internet of things. In Proceedings of the IASTED International Conference on Engineering and Applied Science, EAS 2012 Dec (pp. 84-90).

[127] Hong N. A security framework for the internet of things based on public key infrastructure. In Advanced Materials Research 2013 (Vol. 671, pp. 3223-3226). Trans Tech Publications Ltd.

[128] Nyangaresi VO, Abduljabbar ZA, Ma J, and Sibahee MAA. Temporary Symmetric Key Based Message Verification Protocol for Smart Energy Networks. In 2022 IEEE 7th International Energy Conference (ENERGYCON) 2022 July (pp. 1-6). IEEE.

[129] Karthikeyan S, Patan R, Balamurugan B. Enhancement of security in the Internet of Things (IoT) by using X. 509 authentication mechanism. In Recent Trends in Communication, Computing, and Electronics 2019 (pp. 217-225). Springer, Singapore.

[130] Durairaj M, Muthuramalingam K. A new authentication scheme with elliptical curve cryptography for internet of things (IoT) environments. Int. J. Eng. Technol. 2018;7(2.26):119-24.

[131] Nyakomitta SP, Omollo V. Biometric-Based Authentication Model for E-Card Payment Technology. IOSR Journal of Computer Engineering (IOSRJCE). 2014;16(5):137-44.

[132] Alotaibi M. An enhanced symmetric cryptosystem and biometric-based anonymous user authentication and session key establishment scheme for WSN. IEEE Access. 2018 Nov 9; 6:70072-87.

[133] Park N, Kang N. Mutual authentication scheme in secure internet of things technology for comfortable lifestyle. Sensors. 2015 Dec 24; 16(1):20.

[134] Nyangaresi VO, Abduljabbar ZA, Sibahee MA, Abood EW, Abduljaleel IQ. Dynamic Ephemeral and Session Key Generation Protocol for Next Generation Smart Grids. InAd Hoc Networks and Tools for IT 2021 Dec 6 (pp. 188-204). Springer, Cham.

[135] Shao J, Lu R, Lin X, Zuo C. New threshold anonymous authentication for VANETs. In 2015 IEEE/CIC International Conference on Communications in China (ICCC) 2015 Nov 2 (pp. 1-6). IEEE.

[136] Shao J, Lin X, Lu R, Zuo C. A threshold anonymous authentication protocol for VANETs. IEEE Transactions on vehicular technology. 2015 Feb 24; 65(3):1711-20.

[137] Lai C, Lu R, Zheng D, Li H, Shen XS. GLARM: Group-based lightweight authentication scheme for resource-constrained machine to machine communications. Computer Networks. 2016 Apr 22; 99:66-81.

[138] Fu A, Lan S, Huang B, Zhu Z, Zhang Y. A novel group-based handover authentication scheme with privacy preservation for mobile WiMAX networks. IEEE Communications Letters. 2012 Sep 19; 16(11):1744-7.

[139] Lai C, Li H, Lu R, Shen XS. SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks. Computer Networks. 2013 Dec 9; 57(17):3492-510.

[140] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[141] Weber RH. Internet of things: Privacy issues revisited. Computer Law & Security Review. 2015 Oct 1; 31(5):618-27.

[142] Emerson S, Choi YK, Hwang DY, Kim KS, Kim KH. An OAuth based authentication mechanism for IoT networks. In2015 International Conference on Information and Communication Technology Convergence (ICTC) 2015 Oct 28 (pp. 1072-1074). IEEE.

[143] Chae CJ, Choi KN, Choi K, Yae YH, Shin Y. The extended authentication protocol using e-mail authentication in OAuth 2.0 protocol for secure granting of user access. Journal of Internet Computing and Services. 2015;16(1):21-8.

[144] Nyangaresi VO, Ibrahim A, Abduljabbar ZA, Hussain MA, Al Sibahee MA, Hussien ZA, Ghrabat MJ. Provably Secure Session Key Agreement Protocol for Unmanned Aerial Vehicles Packet Exchanges. In2021 International Conference on Electrical, Computer and Energy Technologies (ICECET) 2021 Dec 9 (pp. 1-6). IEEE.

[145] Abbasi R, Faseeh Qureshi NM, Hassan H, Saba T, Rehman A, Luo B, Bashir AK. Generalized PVO-based dynamic block reversible data hiding for secure transmission using firefly algorithm. Transactions on Emerging Telecommunications Technologies. 2022 Mar;33(3):e3680.

[146] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In 2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[147] Muhal MA, Luo X, Mahmood Z, Ullah A. Physical unclonable function based authentication scheme for smart devices in Internet of Things. In2018 IEEE International Conference on Smart Internet of Things (SmartIoT) 2018 Aug 17 (pp. 160-165). IEEE.

[148] Nyangaresi VO, Abduljabbar ZA, Refish SH, Al Sibahee MA, Abood EW, Lu S. Anonymous Key Agreement and Mutual Authentication Protocol for Smart Grids. InInternational Conference on Cognitive Radio Oriented Wireless Networks, International Wireless Internet Conference 2022 (pp. 325-340). Springer, Cham.

[149] Vasilomanolakis E, Daubert J, Luthra M, Gazis V, Wiesmaier A, Kikiras P. On the security and privacy of Internet of Things architectures and systems. In 2015 International workshop on secure internet of things (SIoT) 2015 Sep 21 (pp. 49-57). IEEE.

[150] Kumar P, Lee SG, Lee HJ. E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. Sensors. 2012 Feb 7;12(2):1625-47.

[151] Nyangaresi VO, Abood EW, Abduljabbar ZA, Al Sibahe MA. Energy Efficient WSN Sink-Cloud Server Authentication Protocol. In2021 5th International Conference on Information Systems and Computer Networks (ISCON) 2021 Oct 22 (pp. 1-6). IEEE.

[152] Lu JZ, Chen T, Zhou J, Yang J, Jiang J. An enhanced biometrics-based remote user authentication scheme using smart cards. In2013 6th International Congress on Image and Signal Processing (CISP) 2013 Dec 16 (Vol. 3, pp. 1643-1648). IEEE.

[153] Klaokliang N, Teawtim P, Aimtongkham P, So-In C, Niruntasukrat A. A novel IoT authorization architecture on hyperledger fabric with optimal consensus using genetic algorithm. In2018 Seventh ICT International Student Project Conference (ICT-ISPC) 2018 Jul 11 (pp. 1-5). IEEE.

[154] Nyangaresi VO, Khalefa MS, Abduljabbar ZA, Al Sibahee MA. Low Bandwidth and Side-Channeling Resilient Algorithm for Pervasive Computing Systems. InProceedings of International Conference on Communication and Computational Technologies 2023 (pp. 193-208). Springer, Singapore.

[155] Ouaddah A, Elkalam AA, Ouahman AA. Towards a novel privacy-preserving access control model based on blockchain technology in IoT. InEurope and MENA cooperation advances in information and communication technologies 2017 (pp. 523-533). Springer, Cham.

[156] Singh A, Chatterjee K. A secure multi-tier authentication scheme in cloud computing environment. In2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015] 2015 Mar 19 (pp. 1-7). IEEE.

[157] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Aug 23:e13126.

[158] Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed internet of things. Computer Networks. 2013 Jul 5; 57(10):2266-79.

[159] Oriwoh E, Conrad M. ‘Things’ in the Internet of Things: towards a definition. International Journal of Internet of Things. 2015; 4(1):1-5.

[160] Rashid MA, Pajooh HH. A security framework for IoT authentication and authorization based on blockchain technology. In2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) 2019 Aug 5 (pp. 264-271). IEEE.

[161] Panarello A, Tapas N, Merlino G, Longo F, Puliafito A. Blockchain and iot integration: A systematic survey. Sensors. 2018 Aug 6; 18(8):2575.

[162] Nyangaresi VO, Al Sibahee MA, Abduljabbar ZA, Ma J, Khalefa MS. Biometric-Based Packet Validation Scheme for Body Area Network Smart Healthcare Devices. In2022 IEEE 21st Mediterranean Electrotechnical Conference (MELECON) 2022 Jun 14 (pp. 726-731). IEEE.

[163] Pinno OJ, Gregio AR, De Bona LC. Controlchain: Blockchain as a central enabler for access control authorizations in the iot. InGLOBECOM 2017-2017 IEEE Global Communications Conference 2017 Dec 4 (pp. 1-6). IEEE.

[164] Rahulamathavan Y, Phan RC, Rajarajan M, Misra S, Kondoz A. Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption. In2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) 2017 Dec 17 (pp. 1-6). IEEE.

[165] Nyangaresi VO, Abduljabbar ZA, Al Sibahee MA, Abduljaleel IQ, Abood EW. Towards Security and Privacy Preservation in 5G Networks. In2021 29th Telecommunications Forum (TELFOR) 2021 Nov 23 (pp. 1-4). IEEE.

[166] Kshetri N. Can blockchain strengthen the internet of things?. IT professional. 2017 Aug 17; 19(4):68-72.

[167] Ukil A, Bandyopadhyay S, Pal A. IoT-privacy: To be private or not to be private. In 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) 2014 Apr 27 (pp. 123-124). IEEE.

[168] Abood EW, Abdullah AM, Al Sibahe MA, Abduljabbar ZA, Nyangaresi VO, Kalafy SA, Ghrabta MJ. Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics. 2022 Feb 1; 11(1):185-94.

[169] Kalra S, Sood SK. Secure authentication scheme for IoT and cloud servers. Pervasive and Mobile Computing. 2015 Dec 1;24:210-23.

[170] Wu L, Wang J, Choo KK, He D. Secure key agreement and key protection for mobile device user authentication. IEEE Transactions on Information Forensics and Security. 2018 Jun 25;14(2):319-30.

[171] Moon J, Lee D, Jung J, Won D. Improvement of efficient and secure smart card based password authentication scheme. Int. J. Netw. Secur.. 2017 Nov 1;19(6):1053-61.

[172] Abduljabbar ZA, OmolloNyangaresi V, Al Sibahee MA, Ghrabat MJ, Ma J, QaysAbduljaleel I, Aldarwish AJ. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks. 2022 Sep 19;11(3):55.

[173] Mishra D, Chaturvedi A, Mukhopadhyay S. Design of a lightweight two-factor authentication scheme with smart card revocation. Journal of Information Security and Applications. 2015 Aug 1;23:44-53.

[174] Panwar N, Sharma S, Wang G, Mehrotra S, Venkatasubramanian N, Diallo MH, Sani AA. IoT Notary: Sensor data attestation in smart environment. In2019 IEEE 18th International Symposium on Network Computing and Applications (NCA) 2019 Sep 26 (pp. 1-9). IEEE.

[175] Li X, Ibrahim MH, Kumari S, Sangaiah AK, Gupta V, Choo KK. Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. Computer Networks. 2017 Dec 24; 129:429-43.

[176] Chen R, Peng D. Analysis and improvement of a mutual authentication scheme for wireless body area networks. Journal of medical Systems. 2019 Feb; 43(2):1-0.

[177] Pump R, Ahlers V, Koschel A. State of the art in artificial immune-based intrusion detection systems for smart grids. In2018 second world conference on smart trends in systems, security and sustainability (WorldS4) 2018 Oct 30 (pp. 119-126). IEEE.

[178] Chaturvedi A, Mishra D, Jangirala S, Mukhopadhyay S. A privacy preserving biometric-based three-factor remote user authenticated key agreement scheme. Journal of Information Security and Applications. 2017 Feb 1;32:15-26.

[179] [178] Sahoo SS, Mohanty S, Majhi B. A secure three factor based authentication scheme for health care systems using IoT enabled devices. Journal of Ambient Intelligence and Humanized Computing. 2021 Jan; 12(1):1419-34.

[180] Xie Y, Zhang S, Li X, Li Y, Chai Y. Cascp: efficient and secure certificateless authentication scheme for wireless body area networks with conditional privacy-preserving. Security and Communication Networks. 2019 Jun 4; 2019.

[181] Roy M, Chowdhury C, Kundu A, Aslam N. Secure lightweight routing (SLR) strategy for wireless body area networks. In 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) 2017 Dec 17 (pp. 1-4). IEEE