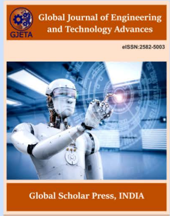
Global Journal of Engineering and Technology Advances

eISSN: 2582-5003

Cross Ref DOI: 10.30574/gjeta

Journal homepage: https://gjeta.com/



(REVIEW ARTICLE)

Check for updates

Secure signaling and traffic exchanges in smart cities: A critical review of the current trends

Catherine Kanini *

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

Global Journal of Engineering and Technology Advances, 2022, 12(03), 026–041

Publication history: Received on 20 July 2022; revised on 14 September 2022; accepted on 16 September 2022

Article DOI: https://doi.org/10.30574/gjeta.2022.12.3.0145

Abstract

The need to enhance convenience, transparency and reduce costs has led to the adoption of smart cities in most countries. In this environment, a myriad of internet of things devices such as sensors and actuators exchange large volumes of highly sensitive and private data. There is therefore need to develop security frameworks, protocols and architectures to offer the much required protection to the exchanged data. To this end, numerous schemes have been put forward by various researchers over the recent past. In this paper, a broad review is provided of the security, privacy and performance issues of these schemes in a smart city environment. Based on the obtained results, it is evident that the attainment of ideal security and privacy for the data exchanged over open wireless channels is an uphill task. Therefore, some recommendations are given on how best the security solutions should be tailored to bridge this gap.

Keywords: Smart city; Security; Privacy; Attacks; Performance; Private

1. Introduction

The Internet of Things (IoT) network offers ubiquitous connection of smart sensors, smart devices and other daily living physical objects, giving rise to smart cities. As such, smart cities provide a platform through which governments deliver real-time unique data to the citizens based on their requirements. Basically, a smart government is the implementation of a set of business processes and enabling information technology that facilitate seamless flow of information across government agencies [1]. The goal is to dispense services in an efficient, cost-effective and transparent manner so as to attain global competitiveness. As explained by Malik et al.[2], the IoT technology in smart cities offer tracking, communication, identification, monitoring, sensing and control functionalities among the numerous physically distributed devices. In addition, the ICT based E-governance has facilitated interactive internet enabled smart delivery of services to the citizens [3]. This delivery is made possible by a range of smart devices which can be implantable or embedded. They may include smart watches, roadside units and smart phones among others [4], [5], [6]. This technology helps alleviate challenges faced by cities such as decreasing state aid, budget declines as well as increased budgetary uncertainty [7], [8].Therefore, smart cities must offer high-quality smart services to the citizens. These services may include environment monitoring, social contact, entertainment, healthcare and transportation. As explained by Zeng et al. [9], the objective of smart systems and services such as smart home, smart appliances, healthcare and monitoring, security and surveillance applications is to enhance convenience in the life of people. In general, smart environments have numerous applications domains such as smart homes [10], smart health care [11], smart grids [12], smart transportation and smart cities [13] as shown in Fig.1.

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

The recent advances in mobile and wireless technologies have enabled citizens to obtain real-time access to data and services, especially in technologically advanced countries [14], [15], [16], [17]. Therefore, smart cities play critical roles in education, economy, tourism and government. To accomplish this, a myriad of electronic gadgets such as cameras, sensors and actuators are deployed [18]. For instance, sensors in smart health systems are capable of measuring blood pressure [19], cardiovascular parameters [20], [21] and respiration variables [22], [23], [24]. On the other hand, sensors and actuators in intelligent transportation improve road safety through the provisioning of more convenient driving experience using dedicated or crowd sensing technologies [25], [26], [27]. For instance, smart parking services facilitate the finding of a suitable vacant parking spot in busy cities [28]. In addition, closed-circuit television camera (CCTV) can be incorporated with IoT to act as smart sensors for enhanced safety and security [18]. In smart homes [29], the smart appliances offer convenience, improve energy consumption through smart heating, ventilation and air conditioning [30]. As explained in [31], the utilization of Cyber Physical Systems (CPSs) in smart cities enhances transportation services, healthcare, utilities, environmental health, utilities and safety. For instance, smart driving employs various technologies to evaluate and assess road status and hence help drivers prevent accidents. Therefore, it contributes to improved drivers and passengers safety [32]. In addition, other intelligent transport systems within the smart city enhance public transportation in addition to offering citywide services that guarantee the smooth flow of traffic [33]. Further, it can help law enforcement officers in addressing traffic incident disputes [34]. In spite of the numerous benefits that accrue from the utilization of smart cities, a number of integrity, authenticity, privacy and security issues [35] are yet to be solved. For instance, although CCTV is a significant element of smart cities [36], they raise a number of integrity issues. This is because of the capabilities of attackers modifying reality so as to spread false information [37]. The many IoT devices supported in smart cities has also been identified in [31] as being the source of vulnerabilities and risks. The increased competition among smart city application developers to introduce novel and innovative products has seen the treatment of security and privacy requirements as afterthoughts [38]. The developers need to meet strict deadlines and therefore they leave security and privacy requirements as elements that can be incorporated later on as system features.

Figure 1 Smart City Elements

Therefore, these immature smart city IoT devices fall short of security and privacy requirements which are critical constituents [39], [40], [41]. Due to the prevalence of many vulnerabilities and attacks in smart city IoT devices, there is a sense of mistrust among the communicating entities [42]. Another serious challenge in these smart cities is the resource-constrained nature of the IoT devices which limits the applicability of strong and enhanced cryptographic techniques [43], [44], [45], [46]. As these IoT systems are being attached to the physical infrastructure systems, there is need to uphold confidentiality, availability and integrity [47]. Unfortunately, the physical layer is the weakest link in these smart city systems as demonstrated by Arias et al. [38], who were able to exploit hardware vulnerabilities to hijack smart home products. Indeed the authors in [48] explain that cryptographic approaches provide only software security and are unable to protect against side-channel and hardware attacks. Particularly, the servers in cloud-based smart city applications have been noted to be vulnerable to attacks such as data leakage [40], malicious data injection, denial of service (DoS) [49] and spoofing. Although techniques such as access control, anonymous communication and encryption can be deployed to protect against these attacks [40], the intrinsic IoT features raise manifold challenges in deploying these off-the-shelf techniques.

Considering smart vehicles, the threats against them can be classified as physical or interception depending on their vulnerabilities [50]. Whereas physical threats target the electronic control unit of vehicles so as to gain unauthorized access to data or sabotage the operation of the vehicle, interception threats aims to capture the exchanged data. Since each vehicle transmits messages containing unique ID and location-related information, eavesdropping attacks can yield critical information about the vehicle and its driver [51]. Similarly, smart grid applications are highly depended on information communication technologies for power line communication, Bluetooth, ZigBee and IEEE 802.11 h [52], [53]. However, making the grid intelligent and integrating it with the cyber world exposes them to numerous vulnerabilities and cyber attacks that can compromise its privacy, integrity and availability [54]. Considering smart homes, security and privacy challenges have been identified in [55] as being major hindrances. As explained by Jose and Malekian [56], smart homes share the weaknesses of wireless local area network protocols. Therefore, they are susceptible to routing and wormhole attacks. In addition, the IoT devices in smart homes are shipped with simple default passwords that users rarely change. Even though strong passwords are deployed, other threats such as firmware and spoofing attacks can still be utilized to compromise the network [57]. By monitoring the IP addresses of the IoT devices or using machine learning techniques, it becomes easy for attackers to trace data packets to their source devices. It is also possible to eavesdrop the communication channel and hence compromise user privacy. Therefore, smart devices should be made anonymous and techniques for preempting unauthorized data fusion should be incorporated [58].

Based on the discussion above, it is clear that IoT nodes in smart cities can be compromised and hence endanger public safety. Any successful attack can have devastating impact due to the high number of devices involved. As such, security smart cities safety is important. Unfortunately, IoT-based smart cities are vulnerable to unauthorized access [59], [60]. Technologies such as artificial intelligence, virtual reality, botnets and smart vehicles render smart city security assurance extremely challenging [61]. Therefore, upholding privacy and security for data at rest and in transit over smart cities is a challenging task [3], [62], [67], [64], [65], [66]. To curb the threats, strong authentication techniques are needed [67]. For instance, when mobile users request for data services from some remote service providers, the authenticity of each party should be verified [68], [69], [70].

The rest of this paper is organized as follows: Section 2 gives the motivation behind this review, while Section 3 presents the contribution of this study. On the other hand, Section 4 discuses related work, while Section 5 presents the results. Towards the end of this article, Section 6 concludes the paper.

2. Motivation

Large volumes of personal data such as photos, contact details, call logs and bank account details are generated and stored in mobile gadgets such smartphones. Since these smartphones are connected to the smart city IoT communication, the potential threats to the stored information increase exponentially. This is worsened by the fact that smartphones are easily stolen, lost or accessed by non-owners. In addition, in most of the smart city communications, wireless transmission medium is utilized, which is more insecure compared to wired communication channels. Clearly, user privacy is at risk and the entire network is susceptible to attacks such as eavesdropping and forgery. There is therefore a need for proper security solutions.

3. Contributions

The major contributions of this article include the following:

- A broad review of security, privacy and performance issues in smart cities is provided.
- The state-of-the-art security solutions presented in literature are identified.
- The operational shortfalls, security and privacy gaps of the state-of-the-art security solutions are discussed.
- Recommendations geared towards enhanced security and privacy posture in smart cities are provided.

4. Related work

The need to preserve confidentiality, integrity and availability in smart cities has seen the development of many security solutions based on a number of technologies. For instance, user authentication techniques based on passwords and personal identification numbers (PINs) have been presented in literature. Although simple passwords are easy to remember, they are vulnerable to guessing attacks [71], [72]. On the other hand, sophisticated and long passwords are more secure but extremely cumbersome for users to remember [73]. PINs are easily remembered than passwords but are generally less secure and hence can be easily and quickly guessed [74], [75]. Over the recent past, the blockchain technology has been utilized to secure IoT devices in smart cities. For instance, authors in [18], [76], [77], [78] and [79]. Although these schemes enhance trust and prevent forgery attacks, the blockchain technology has high storage and computation costs [80]. To address this challenge, other privacy-preserving authentication (PPA) protocols have been presented in [81], [82], [83], [84], [85] and [86]. Unfortunately, these protocols generally do not provide perfect forward secrecy [87]. To prevent data manipulation over the communication channels and boost trust [88], Intrusion Detection Systems (IDS) have been deployed. This is particularly important in smart transportation where falsified data can mislead drivers resulting in accidents. Game theoretic solutions have also been proposed in distributed architectures such as smart cities [89]. However, their performance depends on various assumptions, such as the rules of the game and whether or not the adversaries are cooperative. Although the scheme in [90] can solve this challenge, it is vulnerable to server impersonation attacks [91], [92]. In addition, the adversary can easily obtain the user's genuine identity.

Hybrid machine learning based techniques have also been instrumental in smart city security, more so in anomaly detection [93]. However, the efficacy of these algorithms relies on feature extraction, which present some challenges. For instance, salient features extraction is a complicated task. In addition, adversaries can learn the relevant features and engineer their attacks accordingly [94]. Since deep learning (DL) techniques operate on raw data, they can be deployed to solve this problem. In addition, DL based IDS have been shown to be resilient against zero-day attacks owing to their tolerance to small changes in data compared to other machine learning algorithms [95]. Unfortunately, DL algorithms call for large and high-quality training datasets [96]. Biometric technology presents another significant method for enhancing smart city security. For instance, a biometrics-based authentication and key agreement protocol has been presented by Yoon and Yoo [97]. However, this scheme is susceptible to user impersonation attacks [98], [99]. Similarly, authors in [100] have identified some flaws in the scheme developed by He and Wang [101]. In addition, the protocols in [100] and [101] require the registration center (RC) to be always online to facilitate mutual authentication. Therefore, these approaches cannot scale well and incur high costs in establishing and maintaining an always online RC.

In smart transportation, location based services are critical for the provision of context-sensitive information. However, this raises privacy concerns especially when adversaries access the location data. Most of the existing user location preserving solutions have high computation and communication. Although pseudonyms are widely deployed for location privacy protection, their management is centralized. This raises concerns about scalability and communication latencies as the number of devices surge. To address this problem, there is need for distributed pseudonym management systems that employ edge computing [102]. To prevent video forgery in smart cities CCTV, a scheme employing recurrent neural networks is proposed in [103]. On the other hand, a scheme using bilinear paring operation during the authentication phase is introduced in [91]. However, these pairing operations are time consuming [104]. Similarly, digital videos trustworthiness identification model is presented in [105], while a video authentication technique is presented in [106]. To enhance integrity of stored sensor logs, a verification technique is introduced in [107]. However, the efficacy of this approach is depended on the deployed instrument. This challenge is addressed by the schemes in [108] and [109]. Standard cryptographic approaches such as transport layer security (TLS) and secure socket layer (SSL) can also be utilized to enhance privacy and security in smart cities. However, these approaches are quite expensive for resource-constrained IoT devices [110]. This challenge can be addressed by lightweight key-establishment mechanisms based on symmetric encryption in [111].

To increase integrity, a verification strategy is presented in [112]. Unfortunately, the authors failed to discuss the spectrum and implementation details of this approach. To detect irregular energy consumption, ML and DL have been deployed in [113]. Although this scheme has impressive accuracy, it requires high-quality training data. Artificial immune systems can also be deployed here, but their applicability to real-world scenarios is not completely known [114]. A watermark based CCTV video authentication method is presented in [115]. However, this technique cannot protect against forgery. Further, new nodes and participants additions as well as their verification procedures [116] are not discussed. These issues can be addressed by the scheme in [117]. However, this approach fails to offer forward secrecy [118], [119]. On the other hand, Trusted Platform Module (TPM) based hardware and software security implementations have high power and cost overheads [120]. There is therefore need to develop IoT-optimized integrity attestation schemes that do not rely on TPM [121]. For instance, the schemes in [122] and [123] do not require TPM. However, the scheme in [122] is not robust against password guessing and smart card loss attacks. Similarly, the scheme in [124] is vulnerable to password guessing attacks [125]. Therefore, improved schemes are presented in [126] and [127].

The physically unclonable functions (PUFs) present another technology that can be utilized to secure smart city IoT devices against physical attacks. However, the challenge-response pairs can sometimes be inconsistent, raising stability issues [128], [129]. To curb this, the biometric authentication scheme in [130] can be deployed. Encryption algorithms can also help in securing smart cities through authenticity validation and spoofing detection [131]. Unfortunately, these algorithms can never defend against side-channel attacks. In addition, most of these encryption techniques have high computation overheads [132]. Although the scheme in [125] can alleviate side-channeling attacks, it cannot defend against user impersonation and password guessing attacks [133]. To address password guessing and impersonation attacks [134], physiological and behavioral biometric authentication schemes have been presented in [135], [136], [137], [138], [139], [140], [141], [142], [143]. However, physiological biometrics based authentications using iris recognition, face locks and fingerprint scans can be duplicated and changed. For instance, hand geometry and fingerprints can be recreated in plastic, while scars and bruises can alter the fingerprints. In addition, diverse face poses can confuse face recognition systems. Further, physiological biometric techniques using fingerprint and iris recognition call for additional hardware for input. These challenges can be addressed by behavioral biometric authentication schemes such as the one developed in [139]. Moreover, the protocol developed in [144] can also mitigate some of these issues. However, this method does not offer forward key secrecy and is vulnerable to smart card loss attacks [145], [146].

Fully homomorphic encryption techniques such as the ones in [147] and [148] can enable servers apply algorithms to encrypted data without first requiring them to be decrypted. However, current homomorphic algorithms have significant performance penalty that render them unsuitable for many smart city applications. In addition, these schemes cannot protect against hardware and side-channel threats such as cache, timing and power analysis attacks [48]. Therefore, improved schemes based on Elliptic Curve Cryptography (ECC) and pseudonyms are proposed in [149] and [131] respectively. However, the ECC in [149] increases the size of the exchanged messages. On the other hand, pseudonyms [150] may make it difficult to identify malicious users in the networks. This problem can be solved using identity based protocols in [151] and [152]. However, identity-based schemes have key escrow issues [153]. Therefore, an improved scheme is presented in [154], which is shown to resist key exposure attacks.

Attribute based encryption (ABE) algorithms are effective in the provision of diverse access control privileges. This renders them applicable in cloud-based smart cities. However, ABE has high computation complexity [155] which is unsuitable for IoT devices. In addition, both ABE and identity-based protocols require central servers, which limit their applicability in distributed implementations. To solve this challenge, Certificateless Signcryption (SLSC) technique has been introduced in [156]. In these techniques, the service provider only dispenses partial keys, eliminating the need for a completely trustful server. Similarly, smart card based remote user authentication scheme in [157] incurs low computational costs and hence can address the issues in ABE based schemes. Blockchain technology based schemes have been deployed to uphold non-repudiation and eliminate central server requirements [158], [159], [160], [161]. However, these blockchain based protocols are vulnerable to 51% attacks. In addition, they have high storage and computation complexities [162]. These complexities result in high latencies which cause inconvenience for users [163]. Since blockchain enables the tracking of user transactions, their visiting patterns can be revealed, compromising their privacy.

5. Results and discussion

The extensive literature review carried out has yielded many security solutions tailored for the smart cities. These security solutions are based on techniques such as blockchain, identity, attributes, biometrics, PUFs, watermarking, smart cards, TPM, fully homomorphic, ECC, game theory, machine learning, passwords and PINs. Table 1 presents the observed weaknesses of these techniques.

Table 1 Smart Cities Security Techniques Challenges

Technique	Challenges
Passwords and PINs	Vulnerable to guessing attacks; cumbersome for users to remembers
Blockchain	Susceptible to 51% attacks; high storage and computation costs
Game theory	Performance depends on various assumptions, such as the rules of the game and whether or not the adversaries are cooperative
Machine learning	Salient features extraction is a complicated task; adversaries can learn the relevant features and engineer their attacks accordingly

Biometric	Can be duplicated and changed; fingerprints can be recreated in plastic
TLS, SSL	Expensive for resource-constrained IoT devices
Watermarking	Cannot protect against forgery
TPM	High power and cost overheads
PUF	Have stability issues
Fully homomorphic	Have significant performance penalty
ECC	High bandwidth requirements
Identities	Have key escrow issues
ABE	High computation complexity; inapplicable in distributed implementations
Smart card	Prone to smart card loss and side-channel attacks

As shown in Table 1, all these technologies have either security or privacy issues. There is therefore need to explore novel technologies that can sufficiently protect smart cities. Table 2 presents the challenges of the specific smart cities security approaches.

Table 2 Challenges of Smart Cities Security Schemes

Scheme	Weaknesses
Gipp et al. [76], Khan et al. [18] Kim et al. [77], Javaid et al. [78], Hang et al. [79]	High storage and computation costs
Sood et al. [81], Lee et al. [82], Tsaur et al. [83], Mishra et al. [84], Li et al. [85], Xue et al. [86]	Lack perfect forward secrecy
Tsai and Lo [90]	Vulnerable to server impersonation attacks; adversary can easily obtain the user's real identity
Aloqaily et al. [93]	Salient features extraction is a complicated task; adversaries can learn the relevant features and engineer their attacks accordingly
Yoon and Yoo [97]	Susceptible to user impersonation attacks
Odelu et al.[100] , He and Wang [101]	Require an online RC; has scalability issues; incur high costs
He et al. [91]	Time consuming
Ghimire et al. [112]	Spectrum and implementation details are not discussed
Yip et al. [113]	Requires high-quality training data
Kerr et al. [115]	Cannot protect against forgery
Chen et al. [117]	Fails to offer forward secrecy
Kumari et al. [122]	Susceptible to password guessing and smart card loss attacks

Chen et al. [124]	Vulnerable to password guessing attacks
Jiang et al. [125]	Defenseless against user impersonation and password guessing attacks
Dhillon and Kalra [135], Frank et al. [136], Trojahn et al. [137], Chaturvedi et al. [138], Zheng et al. [139], Ferrero et al. [141], Nickel et al. [142], [Buthpitiya et al. [143]	Deployed features can be duplicated and altered
Shunmuganathan et al. [144]	Cannot offer forward key secrecy; is vulnerable to smart card loss attacks
Honan et al. [147], Page et al. [148]	Have significant performance penalty; cannot protect against hardware and side-channel threats
Kalra and Sood [149]	High bandwidth requirement; difficult to identify malicious users in the network
Chaudhry et al. [151], [Zhong et al. [152]	Have key escrow issues
Hammi et al. [158], [Rathee et al. [159], [Ouaddah et al. [160], [Rashid et al. [161]	Vulnerable to 51% attacks; can compromise user privacy

As shown in Table 2, all these schemes have security issues that can potentially impede their applicability in smart cities. Therefore, the recommendations in Section 6 are deemed necessary in addressing some of these challenges.

Recommendations

From the foregoing discussions, it is obvious that smart cities face numerous security challenges. Although a good number of schemes have been presented in literature, perfect security at low complexities remains a mirage. For instance, three-factor authentication using biometrics, passwords and smart cards has been shown to be effective [164], [165]. However, this authentication is complicated and hence prohibitive for some smart city users such as the elderly and disabled. In addition, continuous authentications cannot be provided by these three-factor based schemes. There is therefore need for non-invasive and user-friendly authentication approaches for every communication channel as shown in Fig.2. To accomplish this, information collected by radio frequency sensors, cameras and radio frequency identification systems [166] can be deployed.

Most of the conventional smart city security solutions involve public and private key pairs. Consequently, they require an additional copy of data for every data access request [48]. Therefore, for smart city application scenario such as smart healthcare with complicated data access patterns, these solutions can become prohibitively sophisticated. There is therefore need for less sophisticated authentication schemes that provide the same level of protection.

To address the resource-constrained nature of smart city IoT devices, many lightweight key-establishment techniques based on symmetric encryption have been presented. Unfortunately, most of these approaches rely on trusted centralized authorities which are assumed to be tamper-proof. However, this assumption does not hold in most smart city application domains. In addition, encryption can potentially complicate data query and data processing [167]. Therefore, a need arises for innovative approaches of making data query and processing efficient in the face of symmetric encryption.

Figure 2 Proposed Smart City Secure Message Exchanges

6. Conclusion

This paper has discussed the privacy, security and performance of the current schemes developed for securing the smart city environment. It has been shown that most of the current security solutions have numerous security gaps that require immediate attention. In addition, performance is another major hindrance for the utilization of majority of these schemes in resource-constrained IoT environments such as smart cities. Based on the identified gaps, a number of recommendations are given which are thought to be necessary for the attainment of perfect security in smart cities. Future work will include the practical implementations of these recommendations so that their effect on security and performance can be empirically analyzed.

Compliance with ethical standards

Acknowledgments

I would like to express my gratitude to all my colleagues and faculty members who made the completion of this paper successful.

References

[1] Rokhman A. e-Government adoption in developing countries; the case of Indonesia. Journal of Emerging Trends in Computing and Information Sciences. 2011 May;2(5):228-36.

[2] Malik MN, Azam MA, Ehatisham-Ul-Haq M, Ejaz W, Khalid A. ADLAuth: Passive authentication based on activity of daily living using heterogeneous sensing in smart cities. Sensors. 2019 May 29;19(11):2466.

[3] Sharma G, Kalra S. Advanced multi-factor user authentication scheme for E-governance applications in smart cities. International Journal of Computers and Applications. 2019 Jul 4;41(4):312-27.

[4] Taleb T, Dutta S, Ksentini A, Iqbal M, Flinck H. Mobile edge computing potential in making cities smarter. IEEE Communications Magazine. 2017 Mar 13;55(3):38-43.

[5] Li J, Zhang W, Kumari S, Choo KK, Hogrefe D. Security analysis and improvement of a mutual authentication and key agreement solution for wireless sensor networks using chaotic maps. Transactions on Emerging Telecommunications Technologies. 2018 Jun;29(6):e3295.

[6] Nyangaresi VO, Rodrigues AJ, Abeka SO. Efficient group authentication protocol for secure 5G enabled vehicular communications. In 2020 16th International Computer Engineering Conference (ICENCO) 2020 Dec 29 (pp. 25-30). IEEE.

[7] Maciag M, Wogan JB. With less state aid, localities look for ways to cope. Governing. 2017 Feb 7;30:32-7.

[8] Pagano M, Hoene CW. City Budgets in an Era of Increased Uncertainty. Metropolitan Policy Program at Brookings. 2018 Jul.

[9] Zeng E, Mare S, Roesner F. End user security and privacy concerns with smart homes. In Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017) 2017 (pp. 65-80).

[10] Caragliu A, Del Bo C, Nijkamp P. Smart cities in Europe. InSmart cities 2013 Aug 22 (pp. 185-207). Routledge.

[11] Demirkan H. A smart healthcare systems framework. It Professional. 2013 May 14;15(5):38-45.

[12] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[13] Chourabi H, Nam T, Walker S, Gil-Garcia JR, Mellouli S, Nahon K, Pardo TA, Scholl HJ. Understanding smart cities: An integrative framework. In2012 45th Hawaii international conference on system sciences 2012 Jan 4 (pp. 2289-2297). IEEE.

[14] Dhillon HS, Huang H, Viswanathan H. Wide-area wireless communication challenges for the Internet of Things. IEEE Communications Magazine. 2017 Feb 3;55(2):168-74.

[15] Qiu T, Chen N, Li K, Qiao D, Fu Z. Heterogeneous ad hoc networks: Architectures, advances and challenges. Ad Hoc Networks. 2017 Feb 1;55:143-52.

[16] Stefanizzi ML, Mottola L, Mainetti L, Patrono L. COIN: Opening the internet of things to people's mobile devices. IEEE Communications Magazine. 2017 Feb 3;55(2):20-6.

[17] 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.

[18] Khan PW, Byun YC, Park N. A data verification system for CCTV surveillance cameras using blockchain technology in smart cities. Electronics. 2020 Mar 15;9(3):484.

[19] Kachuee M, Kiani MM, Mohammadzade H, Shabany M. Cuffless blood pressure estimation algorithms for continuous health-care monitoring. IEEE Transactions on Biomedical Engineering. 2016 Jun 14;64(4):859-69.

[20] Mahbub I, Pullano SA, Wang H, Islam SK, Fiorillo AS, To G, Mahfouz MR. A low-power wireless piezoelectric sensor-based respiration monitoring system realized in CMOS process. IEEE Sensors Journal. 2017 Jan 10;17(6):1858-64.

[21] Rachim VP, Chung WY. Wearable noncontact armband for mobile ECG monitoring system. IEEE transactions on biomedical circuits and systems. 2016 May 18;10(6):1112-8.

[22] Liu X, Cao J, Tang S, Wen J, Guo P. Contactless respiration monitoring via off-the-shelf WiFi devices. IEEE Transactions on Mobile Computing. 2015 Dec 3;15(10):2466-79.

[23] 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.

[24] Reyes BA, Reljin N, Kong Y, Nam Y, Chon KH. Tidal volume and instantaneous respiration rate estimation using a volumetric surrogate signal acquired via a smartphone camera. IEEE journal of biomedical and health informatics. 2016 Feb 25;21(3):764-77.

[25] Habibzadeh H, Qin Z, Soyata T, Kantarci B. Large-scale distributed dedicated-and non-dedicated smart city sensing systems. IEEE Sensors Journal. 2017 Jul 11;17(23):7649-58.

[26] Datondji SR, Dupuis Y, Subirats P, Vasseur P. A survey of vision-based traffic monitoring of road intersections. IEEE transactions on intelligent transportation systems. 2016 Apr 22;17(10):2681-98.

[27] Calabrese F, Colonna M, Lovisolo P, Parata D, Ratti C. Real-time urban monitoring using cell phones: A case study in Rome. IEEE transactions on intelligent transportation systems. 2010 Oct 4;12(1):141-51.

[28] Chatzigiannakis I, Vitaletti A, Pyrgelis A. A privacy-preserving smart parking system using an IoT elliptic curve based security platform. Computer Communications. 2016 Sep 1;89:165-77.

[29] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Sep;3(5):1-6.

[30] Yan J, Zeng Q, Liang Y, He L, Li Z. Modeling and implementation of electroactive smart air-conditioning vent register for personalized HVAC systems. IEEE Access. 2017 Feb 6;5:1649-57.

[31] Habibzadeh H, Nussbaum BH, Anjomshoa F, Kantarci B, Soyata T. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustainable Cities and Society. 2019 Oct 1;50:101660.

[32] Teichmann M, Weber M, Zoellner M, Cipolla R, Urtasun R. Multinet: Real-time joint semantic reasoning for autonomous driving. In2018 IEEE intelligent vehicles symposium (IV) 2018 Jun 26 (pp. 1013-1020). IEEE.

[33] Brisimi TS, Cassandras CG, Osgood C, Paschalidis IC, Zhang Y. Sensing and classifying roadway obstacles in smart cities: The street bump system. IEEE Access. 2016 Feb 11;4:1301-12.

[34] Wu HT, Horng GJ. Establishing an intelligent transportation system with a network security mechanism in an Internet of vehicle environment. Ieee Access. 2017 Sep 14;5:19239-47.

[35] Nyangaresi VO. ECC based authentication scheme for smart homes. In2021 International Symposium ELMAR 2021 Sep 13 (pp. 5-10). IEEE.

[36] Talari S, Shafie-Khah M, Siano P, Loia V, Tommasetti A, Catalão JP. A review of smart cities based on the internet of things concept. Energies. 2017 Mar 23;10(4):421.

[37] Li Y, Lyu S. Exposing deepfake videos by detecting face warping artifacts. arXiv preprint arXiv:1811.00656. 2018 Nov 1.

[38] Arias O, Wurm J, Hoang K, Jin Y. Privacy and security in internet of things and wearable devices. IEEE Transactions on Multi-Scale Computing Systems. 2015 Nov 6;1(2):99-109.

[39] Khatoun R, Zeadally S. Cybersecurity and privacy solutions in smart cities. IEEE Communications Magazine. 2017 Mar 13;55(3):51-9.

[40] Zhang K, Ni J, Yang K, Liang X, Ren J, Shen XS. Security and privacy in smart city applications: Challenges and solutions. IEEE Communications Magazine. 2017 Jan 19;55(1):122-9.

[41] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[42] Angrishi K. Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets. arXiv preprint arXiv:1702.03681. 2017 Feb 13.

[43] Soyata T, Copeland L, Heinzelman W. RF energy harvesting for embedded systems: A survey of tradeoffs and methodology. IEEE Circuits and Systems Magazine. 2016 Feb 11;16(1):22-57.

[44] Shishvan OR, Zois DS, Soyata T. Machine intelligence in healthcare and medical cyber physical systems: A survey. IEEE Access. 2018 Aug 20;6:46419-94.

[45] Soyata T. GPU parallel program development using CUDA. CRC Press; 2018 Jan 19.

[46] Nyangaresi VO. Provably Secure Protocol for 5G HetNets. In2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2021 Nov 1 (pp. 17-22). IEEE.

[47] Mosenia A, Jha NK. A comprehensive study of security of internet-of-things. IEEE Transactions on emerging topics in computing. 2016 Sep 7;5(4):586-602.

[48] Kocabas O, Soyata T, Aktas MK. Emerging security mechanisms for medical cyber physical systems. IEEE/ACM transactions on computational biology and bioinformatics. 2016 Jan 22;13(3):401-16.

[49] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1;15:100210.

[50] Baig ZA, Szewczyk P, Valli C, Rabadia P, Hannay P, Chernyshev M, Johnstone M, Kerai P, Ibrahim A, Sansurooah K, Syed N. Future challenges for smart cities: Cyber-security and digital forensics. Digital Investigation. 2017 Sep 1;22:3-13.

[51] Rajput U, Abbas F, Eun H, Oh H. A hybrid approach for efficient privacy-preserving authentication in VANET. IEEE Access. 2017 Jun 21;5:12014-30.

[52] Kalalas C, Thrybom L, Alonso-Zarate J. Cellular communications for smart grid neighborhood area networks: A survey. IEEE access. 2016 Apr 7;4:1469-93.

[53] Habibzadeh H, Soyata T, Kantarci B, Boukerche A, Kaptan C. Sensing, communication and security planes: A new challenge for a smart city system design. Computer Networks. 2018 Oct 24;144:163-200.

[54] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[55] Wilson C, Hargreaves T, Hauxwell-Baldwin R. Benefits and risks of smart home technologies. Energy Policy. 2017 Apr 1;103:72-83.

[56] Jose AC, Malekian R. Improving smart home security: Integrating logical sensing into smart home. IEEE Sensors Journal. 2017 May 17;17(13):4269-86.

[57] Ling Z, Luo J, Xu Y, Gao C, Wu K, Fu X. Security vulnerabilities of internet of things: A case study of the smart plug system. IEEE Internet of Things Journal. 2017 May 23;4(6):1899-909.

[58] Kumar P, Braeken A, Gurtov A, Iinatti J, Ha PH. Anonymous secure framework in connected smart home environments. IEEE Transactions on Information Forensics and Security. 2017 Jan 2;12(4):968-79.

[59] Butun I, Erol-Kantarci M, Kantarci B, Song H. Cloud-centric multi-level authentication as a service for secure public safety device networks. IEEE Communications Magazine. 2016 Apr 19;54(4):47-53.

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

[61] Cui L, Xie G, Qu Y, Gao L, Yang Y. Security and privacy in smart cities: Challenges and opportunities. IEEE access. 2018 Jul 11;6:46134-45.

[62] Li J, Zhang W, Dabra V, Choo KK, Kumari S, Hogrefe D. AEP-PPA: An anonymous, efficient and provably-secure privacy-preserving authentication protocol for mobile services in smart cities. Journal of Network and Computer Applications. 2019 May 15;134:52-61.

[63] Papadopoulos EP, Diamantaris M, Papadopoulos P, Petsas T, Ioannidis S, Markatos EP. The long-standing privacy debate: Mobile websites vs mobile apps. InProceedings of the 26th International Conference on World Wide Web 2017 Apr 3 (pp. 153-162).

[64] Li J, Choo KK, Zhang W, Kumari S, Rodrigues JJ, Khan MK, Hogrefe D. EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks. Vehicular Communications. 2018 Jul 1;13:104-13.

[65] Nyangaresi VO, Moundounga AR. Secure Data Exchange Scheme for Smart Grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[66] Mollah MB, Azad MA, Vasilakos A. Security and privacy challenges in mobile cloud computing: Survey and way ahead. Journal of Network and Computer Applications. 2017 Apr 15;84:38-54.

[67] Alzubaidi A, Kalita J. Authentication of smartphone users using behavioral biometrics. IEEE Communications Surveys & Tutorials. 2016 Mar 2;18(3):1998-2026.

[68] Aikat J, Akella A, Chase JS, Juels A, Reiter MK, Ristenpart T, Sekar V, Swift M. Rethinking security in the era of cloud computing. IEEE Security & Privacy. 2017 Jun 9;15(3):60-9.

[69] 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.

[70] Xia Z, Wang X, Sun X, Wang Q. A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. IEEE transactions on parallel and distributed systems. 2015 Feb 11;27(2):340-52.

[71] Kelley PG, Komanduri S, Mazurek ML, Shay R, Vidas T, Bauer L, Christin N, Cranor LF, Lopez J. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In2012 IEEE symposium on security and privacy 2012 May 20 (pp. 523-537). IEEE.

[72] Ma J, Yang W, Luo M, Li N. A study of probabilistic password models. In2014 IEEE Symposium on Security and Privacy 2014 May 18 (pp. 689-704). IEEE.

[73] Owusu E, Han J, Das S, Perrig A, Zhang J. Accessory: password inference using accelerometers on smartphones. Inproceedings of the twelfth workshop on mobile computing systems & applications 2012 Feb 28 (pp. 1-6).

[74] Aviv AJ, Gibson K, Mossop E, Blaze M, Smith JM. Smudge attacks on smartphone touch screens. In4th USENIX Workshop on Offensive Technologies (WOOT 10) 2010.

[75] Schaub F, Deyhle R, Weber M. Password entry usability and shoulder surfing susceptibility on different smartphone platforms. InProceedings of the 11th international conference on mobile and ubiquitous multimedia 2012 Dec 4 (pp. 1-10).

[76] Gipp B, Kosti J, Breitinger C. Securing video integrity using decentralized trusted timestamping on the bitcoin blockchain.

[77] Kim SK, Kim UM, Huh JH. A study on improvement of blockchain application to overcome vulnerability of IoT multiplatform security. Energies. 2019 Jan 27;12(3):402.

[78] Javaid U, Siang AK, Aman MN, Sikdar B. Mitigating loT device based DDoS attacks using blockchain. InProceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems 2018 Jun 15 (pp. 71-76).

[79] Hang L, Kim DH. Reliable task management based on a smart contract for runtime verification of sensing and actuating tasks in IoT environments. Sensors. 2020 Feb 22;20(4):1207..

[80] 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.

[81] Sood SK, Sarje AK, Singh K. A secure dynamic identity based authentication protocol for multi-server architecture. Journal of Network and Computer Applications. 2011 Mar 1;34(2):609-18.

[82] Lee CC, Lin TH, Chang RX. A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards. Expert Systems with Applications. 2011 Oct 1;38(11):13863-70.

[83] Tsaur WJ, Li JH, Lee WB. An efficient and secure multi-server authentication scheme with key agreement. Journal of Systems and Software. 2012 Apr 1;85(4):876-82.

[84] Mishra D, Das AK, Mukhopadhyay S. A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards. Expert Systems with Applications. 2014 Dec 15;41(18):8129-43.

[85] Li X, Xiong Y, Ma J, Wang W. An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards. Journal of Network and Computer Applications. 2012 Mar 1;35(2):763-9.

[86] Xue K, Hong P, Ma C. A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture. Journal of Computer and System Sciences. 2014 Feb 1;80(1):195-206.

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

[88] Guo L, Dong M, Ota K, Li Q, Ye T, Wu J, Li J. A secure mechanism for big data collection in large scale internet of vehicle. IEEE Internet of Things Journal. 2017 Mar 22;4(2):601-10.

[89] Sedjelmaci H, Hadji M, Ansari N. Cyber security game for intelligent transportation systems. IEEE Network. 2019 Jan 25;33(4):216-22.

[90] Tsai JL, Lo NW. A privacy-aware authentication scheme for distributed mobile cloud computing services. IEEE systems journal. 2015 May 21;9(3):805-15.

[91] He D, Kumar N, Khan MK, Wang L, Shen J. Efficient privacy-aware authentication scheme for mobile cloud computing services. IEEE Systems Journal. 2016 Dec 28;12(2):1621-31.

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

[93] Aloqaily M, Otoum S, Al Ridhawi I, Jararweh Y. An intrusion detection system for connected vehicles in smart cities. Ad Hoc Networks. 2019 Jul 1;90:101842.

[94] Diro A, Chilamkurti N. Leveraging LSTM networks for attack detection in fog-to-things communications. IEEE Communications Magazine. 2018 Sep 17;56(9):124-30.

[95] Diro AA, Chilamkurti N. Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems. 2018 May 1;82:761-8.

[96] van der Heijden RW, Dietzel S, Leinmüller T, Kargl F. Survey on misbehavior detection in cooperative intelligent transportation systems. IEEE Communications Surveys & Tutorials. 2018 Sep 30;21(1):779-811.

[97] Yoon EJ, Yoo KY. Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem. The Journal of supercomputing. 2013 Jan;63(1):235-55.

[98] 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, (pp.605-612).

[99] Kim H, Jeon W, Lee K, Lee Y, Won D. Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme. InInternational conference on computational science and its applications 2012 Jun 18 (pp. 391-406). Springer, Berlin, Heidelberg.

[100] Odelu V, Das AK, Goswami A. A secure biometrics-based multi-server authentication protocol using smart cards. IEEE Transactions on information forensics and Security. 2015 Jun 1;10(9):1953-66.

[101] He D, Wang D. Robust biometrics-based authentication scheme for multiserver environment. IEEE Systems Journal. 2014 Feb 6;9(3):816-23.

[102] Kang J, Yu R, Huang X, Zhang Y. Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles. IEEE Transactions on Intelligent Transportation Systems. 2017 Nov 10;19(8):2627-37.

[103] Cozzolino D, Poggi G. Autoencoder with recurrent neural networks for video forgery detection Autoencoder with recurrent neural networks for video forgery detection. IS&T Electronic Imaging (EI). 2017.

[104] Nyangaresi VO, Rodrigues AJ, Al Rababah AA. Secure Protocol for Resource-Constrained IoT Device Authentication. International Journal of Interdisciplinary Telecommunications and Networking (IJITN). 2022 Jan 1;14(1):1-5.

[105] Sulaiman N, Bagiwa MA, Aliyu S, Shafii K, Usman AM, Mohammed S, Abdulsalam AJ. Detection and Localization of Splicing Forgery in Digital Videos Using Convolutional Auto-Encoder And Goturn Algorithm. Fudma Journal Of Sciences-ISSN: 2616-1370. 2019 Dec 31;3(4):449-58..

[106] Sowmya KN, Chennamma HR, Rangarajan L. Video authentication using spatio temporal relationship for tampering detection. Journal of Information Security and Applications. 2018 Aug 1;41:159-69..

[107] 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.

[108] Roy A, Karforma S. UML based modeling of ECDSA for secured and smart E-Governance system. InComputer Science & Information Technology (CS & IT-CSCP 2013), Proceedings of National Conference on Advancement of Computing in Engineering Research (ACER13) organized by Global Institute of Management and Technology 2013 Mar 22 (pp. 207-222).

[109] Hoda A, Roy A, Karforma S. Application of ECDSA for security of transaction in E-Governance. InProceedings of Second National Conference on Computing and Systems-2012 (NaCCS-2012) organized by the Department of Computer Science, The University of Burdwan 2012 Mar 15 (pp. 281-286).

[110] 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.

[111] Nyangaresi VO, Abduljabbar ZA, Ma J, Al Sibahee MA. Temporary Symmetric Key Based Message Verification Protocol for Smart Energy Networks. In2022 IEEE 7th International Energy Conference (ENERGYCON) 2022 May 9 (pp. 1-6). IEEE.

[112] Ghimire S, Choi JY, Lee B. Using blockchain for improved video integrity verification. IEEE Transactions on Multimedia. 2019 Jul 1;22(1):108-21.

[113] Yip SC, Wong K, Hew WP, Gan MT, Phan RC, Tan SW. Detection of energy theft and defective smart meters in smart grids using linear regression. International Journal of Electrical Power & Energy Systems. 2017 Oct 1;91:230-40.

[114] 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.

[115] Kerr M, Han F, van Schyndel R. A blockchain implementation for the cataloguing of cctv video evidence. In2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS) 2018 Nov 27 (pp. 1-6). IEEE.

[116] Nyakomitta PS, Nyangaresi VO, Ogara SO. Efficient Authentication Algorithm for Secure Remote Access in Wireless Sensor Networks. Journal of Computer Science Research, 2021 Oct; 3(4), pp. 43-50.

[117] Chen BL, Kuo WC, Wuu LC. Robust smart-card-based remote user password authentication scheme. International Journal of Communication Systems. 2014 Feb;27(2):377-89.

[118] Li X, Niu J, Khan MK, Liao J. An enhanced smart card based remote user password authentication scheme. Journal of Network and Computer Applications. 2013 Sep 1;36(5):1365-71.

[119] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[120] 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.

[121] Broström T, Zhu J, Robucci R, Younis M. IoT boot integrity measuring and reporting. ACM SIGBED Review. 2018 Nov 13;15(5):14-21.

[122] Kumari S, Khan MK, Li X. An improved remote user authentication scheme with key agreement. Computers & Electrical Engineering. 2014 Aug 1;40(6):1997-2012.

[123] 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.

[124] Chen TH, Hsiang HC, Shih WK. Security enhancement on an improvement on two remote user authentication schemes using smart cards. Future Generation Computer Systems. 2011 Apr 1;27(4):377-80.

[125] Jiang Q, Ma J, Li G, Li X. Improvement of robust smart-card-based password authentication scheme. International Journal of Communication Systems. 2015 Jan 25;28(2):383-93.

[126] Sharma G, Kalra S. A novel scheme for data security in cloud computing using quantum cryptography. InProceedings of the International Conference on Advances in Information Communication Technology and Computing, New York, NY, USA (p. 37).

[127] Sharma G, Kalra S. Identity based secure authentication scheme based on quantum key distribution for cloud computing. Peer-to-Peer Networking and applications. 2018 Mar;11(2):220-34.

[128] 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.

[129] Suzuki M, Ueno R, Homma N, Aoki T. Efficient fuzzy extractors based on ternary debiasing method for biased physically unclonable functions. IEEE Transactions on Circuits and Systems I: Regular Papers. 2018 Sep 26;66(2):616-29.

[130] Conti M, Zachia-Zlatea I, Crispo B. Mind how you answer me! Transparently authenticating the user of a smartphone when answering or placing a call. InProceedings of the 6th ACM Symposium on Information, Computer and Communications Security 2011 Mar 22 (pp. 249-259).

[131] Zhou J, Cao Z, Dong X, Vasilakos AV. Security and privacy for cloud-based IoT: Challenges. IEEE Communications Magazine. 2017 Jan 19;55(1):26-33.

[132] 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.

[133] Mishra D, Das AK, Chaturvedi A, Mukhopadhyay S. A secure password-based authentication and key agreement scheme using smart cards. Journal of Information Security and Applications. 2015 Aug 1;23:28-43.

[134] Nyangaresi VO, Abduljabbar ZA, Abduljabbar ZA. Authentication and Key Agreement Protocol for Secure Traffic Signaling in 5G Networks. In2021 IEEE 2nd International Conference on Signal, Control and Communication (SCC) 2021 Dec 20 (pp. 188-193). IEEE.

[135] Dhillon PK, Kalra S. A lightweight biometrics based remote user authentication scheme for IoT services. Journal of Information Security and Applications. 2017 Jun 1;34:255-70.

[136] Frank M, Biedert R, Ma E, Martinovic I, Song D. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE transactions on information forensics and security. 2012 Oct 16;8(1):136-48.

[137] Trojahn M, Ortmeier F. Toward mobile authentication with keystroke dynamics on mobile phones and tablets. In2013 27th International Conference on Advanced Information Networking and Applications Workshops 2013 Mar 25 (pp. 697-702). IEEE.

[138] 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.

[139] Zheng N, Bai K, Huang H, Wang H. You are how you touch: User verification on smartphones via tapping behaviors. In2014 IEEE 22nd International Conference on Network Protocols 2014 Oct 21 (pp. 221-232). IEEE.

[140] 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.

[141] Ferrero R, Gandino F, Montrucchio B, Rebaudengo M, Velasco A, Benkhelifa I. On gait recognition with smartphone accelerometer. In2015 4th Mediterranean Conference on Embedded Computing (MECO) 2015 Jun 14 (pp. 368-373). IEEE.

[142] Nickel C, Wirtl T, Busch C. Authentication of smartphone users based on the way they walk using k-NN algorithm. In2012 Eighth international conference on intelligent information hiding and multimedia signal processing 2012 Jul 18 (pp. 16-20). IEEE.

[143] Buthpitiya S, Zhang Y, Dey AK, Griss M. N-gram geo-trace modeling. InInternational Conference on Pervasive Computing 2011 Jun 12 (pp. 97-114). Springer, Berlin, Heidelberg.

[144] Shunmuganathan S, Saravanan RD, Palanichamy Y. Secure and efficient smart-card-based remote user authentication scheme for multiserver environment. Canadian Journal of Electrical and Computer Engineering. 2015 Mar 30;38(1):20-30.

[145] Irshad A, Sher M, Ashraf S, Hassan MU. Cryptanalysis for secure and efficient smart-card-based remote user authentication scheme for multi-server environment. Cryptology ePrint Archive. 2015.

[146] 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.

[147] Honan G, Page A, Kocabas O, Soyata T, Kantarci B. Internet-of-everything oriented implementation of secure digital health (D-health) systems. In2016 IEEE Symposium on Computers and Communication (ISCC) 2016 Jun 27 (pp. 718-725). IEEE.

[148] Page A, Kocabas O, Soyata T, Aktas M, Couderc JP. Cloud-Based Privacy-Preserving Remote ECG Monitoring and Surveillance. Annals of Noninvasive Electrocardiology. 2015 Jul;20(4):328-37.

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

[150] 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.

[151] Chaudhry SA, Naqvi H, Sher M, Farash MS, Hassan MU. An improved and provably secure privacy preserving authentication protocol for SIP. Peer-to-Peer Networking and Applications. 2017 Jan;10(1):1-5.

[152] Zhong H, Huang B, Cui J, Xu Y, Liu L. Conditional privacy-preserving authentication using registration list in vehicular ad hoc networks. IEEE Access. 2017 Dec 27;6:2241-50.

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

[154] 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.

[155] 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.

[156] Li F, Han Y, Jin C. Cost-effective and anonymous access control for wireless body area networks. IEEE Systems Journal. 2016 May 23;12(1):747-58.

[157] 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.

[158] 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.

[159] 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.

[160] 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.

[161] 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.

[162] 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.

[163] Dagher GG, Mohler J, Milojkovic M, Marella PB. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable cities and society. 2018 May 1;39:283-97.

[164] 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.

[165] Zhang L, Zhu S, Tang S. Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme. IEEE Journal of Biomedical and health informatics. 2016 Jan 12;21(2):465-75.

[166] Kumar T, Braeken A, Liyanage M, Ylianttila M. Identity privacy preserving biometric based authentication scheme for naked healthcare environment. In2017 IEEE international conference on communications (ICC) 2017 May 21 (pp. 1-7). IEEE.

[167] Poh GS, Gope P, Ning J. PrivHome: Privacy-preserving authenticated communication in smart home environment. IEEE Transactions on Dependable and Secure Computing. 2019 May 3;18(3):1095-107.