World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(Review Article)

Check for updates

Cloud computing communication environment security and performance: Challenges and probable solutions

Catherine Kanini *

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

World Journal of Advanced Engineering Technology and Sciences, 2023, 08(01), 110–127

Publication history: Received on 12 December 2022; revised on 24 January 2023; accepted on 26 January 2023

Article DOI: https://doi.org/10.30574/wjaets.2023.8.1.0024

Abstract

The adoption of cloud computing has continued to grow, owing to its broad network access, remote accessibility, scalability, on demand self-service, rapid elasticity and resource pooling. In this environment, numerous devices are deployed to access the cloud data and services. This potentially increases the attack services, more so in public clouds. As such, the biggest challenge is the secure data exchange over insecure open network channels. This issue has seen the development of numerous security solutions over the recent past. In this paper, a survey of these security schemes, techniques and methods is provided. The findings indicate that majority of these methods have vulnerabilities that expose users to many attacks. Additionally, some of these security solutions have extremely high complexities that make the cloud communications inefficient.

Keywords: Algorithms; Authentication; Cloud computing; Security; Storage

1. Introduction

The cloud computing technology involves the distribution of computing resources over the internet. These resources may include storage, network, processing power and applications [1], [2], [3]. The cloud can connect large number of these resources to form an enormous virtually shared resource pool [4]. The aim here is to lower the processing load at user terminals through the exploitation of the cloud's high processing power [5]. Basically, the users access cloud services using any internet-enabled device [6] at any time and from any location. Its other features include broad network access, remote accessibility, scalability, on demand self service, rapid elasticity and resource pooling. These cloud characteristics have enabled the starting of business using little investment costs. The main service models offered by the cloud can be classified as platform as a service (PAAS), infrastructure as a service (IAAS) and software as a service (SAAS) [7]. Storage as a service is another key cloud concept that offers affordability of data access [8] from any location in the globe. According to [9], various organizations utilize three cloud deployment models, which include public, private and hybrid. Among all these models, the public cloud is the cheapest and hence is the most frequently deployed model. The rapid communication and networking technological advancements have increased the popularity of public cloud. As such, many corporations, individuals and businesses have deployed the public cloud to boost their productivity. In a typical communication environment such as the one shown in Figure 1, the computing, communication as well as the storage of most of the Internet of Things (IoT) devices and sensors are limited [10].

As shown in Figure 1, three entities are frequently encountered in a cloud computing environment: the control server, cloud server and clients (users). Here, the cloud server offers the services or data requested by the clients. These requests are sent through various IoT devices that reside at the client side. On its part, the control server is basically some trusted thirty part organization that serves to authorize the clients and the cloud server. This is accomplished through the generation of system parameters during the registration phase. Additionally, the control server monitors

*Corresponding author: Catherine Kanini

the cloud server-client authentication process during client service or data requests. The cloud server and client also establish some session key with the help of the control server. In this environment, numerous devices and sensors need to establish connections with each other and exchange or store massive amounts of information [11]. Cloud computing solves these issues by offering efficient platform to analyze, manage and store the generated IoT data [12], [13].

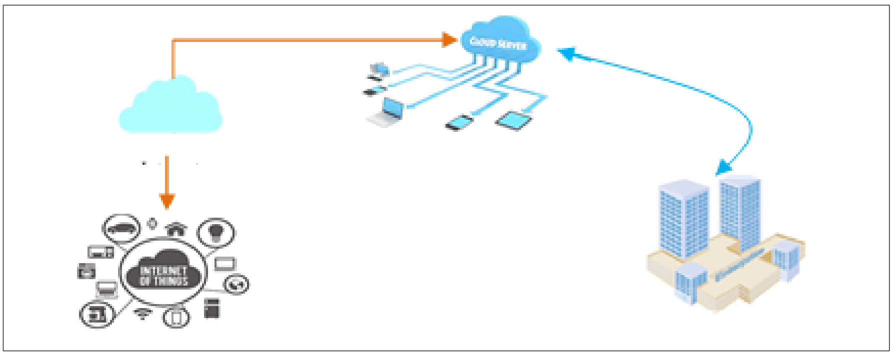

Figure 1 IoT-Cloud Environment

Through the integration of computing resources, the cloud can optimize resource allocation [14]. In the environment, the failure of a particular node will prompt the assignment of its tasks to other nodes. In terms of scalability, the cloud facilitates smooth joining of new nodes to existing computing clusters so as to boost their computing power. This serves to enhance both reliability and efficiency [15]. Despite the cost reductions and increased efficiency, the high number of intelligent IoT devices that must be supported have led to increased latencies, security and privacy violations [16], [17]. For instance, the authors in [18] have surveyed numerous cloud deployments which clearly shows that data sharing lacks protection. In addition, most of the data stored in the cloud is in unencrypted mode [7], [19]. As explained in [20], [21], [22], the data exchange in IoT-enabled cloud computing environments is through public channels. These communication media are open and unprotected and hence there are numerous privacy, tampering and data disclosure issues [23]. As pointed out in [24], bandwidth consumption and service delays are high in the cloud environment characterized by high number of devices. As such, it fails to meet the real-time processing requirements.

To address these issues, robust mutual authentication is required for secure key exchange and online data sharing [25], [26], [27], [28]. This also ensures that there are unique access control procedures and session key establishment before the onset of data sharing, especially in federated cloud environment [29]. Apart from authentication, techniques such as protected credential storage, secure secret key sharing, secure data storage and data sharing have been identified in [30], [31], [32], [33], [34], [35], [36]. As pointed out in [37], [38] and [39], the client data must be encrypted before transmission to and from the cloud servers. To achieve this, both symmetric and asymmetric cryptosystems can be employed. To this end, the contributions of this paper are as follows:

- A detailed review of the cloud environment security and privacy issues is provided.
- A survey of the current cloud protection techniques is offered.
- A comprehensive critique of the conventional security schemes tailored for the cloud computing scenario is carried out.

The rest of this article is structured as follows: In Section 2, cloud computing security solutions that have been put forward in the cloud environment are discussed. However, Section 3 discusses about data sharing techniques in the cloud while Section 4 presents a summary of the findings. This is followed by the Section 5 which offers some guidelines and recommendations which are crucial for the preservation of security in the cloud environment. Finally, Section 6 concludes this paper and offers some insights into future work.

2. Security schemes for cloud environment

Many techniques have been presented in literature to offer privacy and privacy enhancement in cloud computing. For instance, a cloud-based RFID authentication scheme is developed in [40]. Unfortunately, this approach has excessive execution overheads due to the employed quadratic residual that require extensive computations. As such, the efficiency of this scheme is low. Other researchers have also deployed quick response (QR) codes [41] to address cloud computing security challenges while authors in [42], [43], [44] and [45] have presented cloud computing authentication protocols. However, these protocols cannot offer perfect forward security. In addition, they are vulnerable to from man-in-the-middle (MITM) and temporary value disclosure attacks [46]. Specifically, the lightweight AKA scheme for cloud computing introduced in [42] is susceptible to impersonation and session key exposure attacks. It also fails to offer strong mutual authentication [47]. On its part, the scheme in [44] cannot provide perfect forward security. It can also not protect against packet replays, impersonation, and temporary value disclosure attacks [48], [49]. Similarly, the scheme in [45] is unable to resist offline password guessing attacks [50]. Based on radio-frequency identification (RFID), an authentication protocol for cloud environment is introduced in [51], while an anonymous authentication technique is proposed in [52]. However, these two schemes have high computation costs [53] at the tag side. Although the scheme in [54] can address this issue, it fails to protect against impersonation attacks. In addition, it cannot achieve perfect forward key secrecy.

Based on user identities (IDs) and one time password (OTP) verification procedures, a two-factor authentication protocol is developed in [7]. However, simple and cacheable passwords render this scheme insecure. In addition, the usage of same credentials across many devices can render it vulnerable to guessing and dictionary attacks [27]. Although authentication protocols such as FIDO, Kerberos, OAuth and Open ID play critical roles in cloud –based services, their usage of static user identities render them susceptible to tracking attacks [55]. Therefore, a novel scheme is presented in [56] to alleviate this challenge. Unfortunately, this method is susceptible to known session key disclosure attacks. It also fails to achieve perfect forward key secrecy [57]. Therefore, RSA-based scheme is introduced in [35] while an elliptic curve cryptography (ECC) based scheme is presented in [36]. However, the technique in [36] requires some trusted authority (TA) which can present some single point of failure. In addition, the TA has knowledge of the private keys of the users and hence this scheme is vulnerable to privileged insider attacks [32]. Similarly, the scheme in [58] relies on TA [59] [60] and hence faces the same fate as the approach in [36]. This issue is addressed by the ECC-based protocol developed in [61]. Although this approach fulfills numerous security requirements, it cannot protect against packet replay attacks. In addition, it fails to offer perfect forward secrecy.

To offer enhanced efficiency, a lightweight authentication protocol is introduced in [62] based on recursive hash functions. Unfortunately, this method is susceptible to de-synchronization attacks and replay attacks [63]. On the other hand, auditable pseudonym based authentication schemes are developed in [64], [65], [66], [67], [68], [69], [70], [71] to enhance user anonymity. On the flip-side, the scheme in [64] relies on TA while the technique in [65] requires a trusted third party (TTP) to store all the users' private keys. This renders it vulnerable to attacks such as user impersonation and key tampering. On its part, the protocol in [67] employs consortium blockchain which makes it inefficient [72]. Similarly, the conditional privacy based scheme in [69] offers anonymous authentication with the cloud service provider but at the expense of increased overheads. Although the schemes in [64], [65], [66], [67], [69], [70], [71] offer user anonymity, their reliance on trusted third parties to recover the user real identity exposes them to single point of failure. This problem can be tackled by the bilinear pairing based protocol in [73]. However, the architecture of this scheme lacks both the user registration and revocation phases [74].

Based on left rotation function Rots, an authentication method is developed in [75]. Unfortunately, this technique cannot defend against de-synchronization and tracking attacks [76]. On the other hand, a smart-card based scheme is introduced in [77] for a multi-server environment. However, this approach cannot protect against impersonation, traceability, and spoofing and session key disclosure attacks. On its part, the protocol in [78] is vulnerable to impersonation and session key disclosure attacks. In addition, its password change phase is insecure. Similarly, the protocol in [79] is susceptible to privileged insider and offline password guessing attacks. On its part, the protocol in [80] cannot offer untraceability and anonymity [81]. Based on ensemble voting classifier, ECC and Schnorr's signature, a mutual authentication scheme is developed in [29] to detect and mitigate security breaches. On the other hand, the protocol in [82] is defenseless against secret key guessing attacks. As such, the user and cloud server can be easily compromised. Similarly, the schemes in [83], [84] cannot protect against secret key guessing attacks. Based on the blockchain technology, an anonymous user authentication technique is developed in [55] for cloud services. However, the deployed blockchain technology is storage and computationally extensive [85]. On the other hand, an ECC-based protocol is presented in [86]. Unfortunately, this technique is susceptible to impersonation and offline password guessing attacks. In addition, it fails to ensure anonymity of the entities during the authentication process. Similarly, the lightweight authentication scheme in [87] is efficient but fails to defend against packet replay attacks [88]. On its part, the scheme in [89] cannot defend against user impersonation and session key disclosure attacks. In addition, it cannot provide user anonymity [90]. Therefore, the authors in [90] have developed a protocol that is shown to protect against temporary value disclosure, privileged insider, offline password guessing and replay attacks [91]. However, this scheme cannot protect against impersonation attacks [92]. These issues can be effectively tackled by the scheme in [74].

Using blind signatures, key agreement techniques are developed in [93], [94]. Although the authors claim that these two techniques can prevent numerous attacks, they are defenseless against reflection attacks [95]. Similarly, a blind signature based key agreement authentication scheme is developed in [96]. Unfortunately, this protocol cannot provide efficient malicious user revocation. Therefore, a novel authentication protocol is developed in [97]. However, this approach cannot withstand denial of service attacks (DoS) and sensor capture attacks. It can also not offer perfect forward security [98]. Similarly, the protocol in [99] cannot defend against impersonation, man-in-the middle, de-synchronization, session key disclosure and offline password guessing attacks. It can also not offer anonymity and perfect forward secrecy. Therefore, the authors in [100] present a modular exponentiation operation based protocol. However, this approach is inefficient due to extensive hashing operations [101]. Based on physically unclonable function (PUF), a cloud-based RFID scheme is presented in [102]. Similarly, PUF-based protocols are developed in [103], [104], [105], [106]. Although the scheme in [102] is efficient and trustworthy, PUF-based schemes have stability challenges. Similarly, the approach in [107] is susceptible to password guessing and impersonation attacks [108]. Additionally, it cannot ensure perfect forward secrecy. Although the scheme in [109] tackles this challenge, it requires the execution of multiple hashing function operations during data protection and hence is computationally inefficient. Using HTTP cookies and ECC, a mutual authentication protocol is presented in [110] for cloud service providers and IoT devices. Although this technique is robust against replay, man in-the-middle, offline dictionary and cookie theft attacks, point multiplication over ECC may lead to high computation overheads [111].

To address scalability and time constraints, a cloud-centric authentication scheme is developed in [112] while public and private keys based protocols are presented in [32], [36]. On the other hand, an ECC-based scheme is developed in [113]. Unfortunately, this approach is susceptible to session key disclosure, impersonation, man-in-the-middle and offline password guessing attacks. Similarly, the scheme in [114] cannot provide perfect forward secrecy and is defenseless against impersonation and offline password guessing attacks [115]. To address this issue, ECC and bilinear pairing based protocols are developed in [116] and [117]. Unfortunately, are inefficient for authenticating IoT devices to the cloud infrastructure [118]. Similarly, a bilinear pairing based anonymous authentication scheme is introduced in [119] for the cloud computing environments. Unfortunately, this protocol cannot withstand server impersonation attacks [120]. In addition, the deployed pairing operations increase its execution time [121]. Based on static pseudonyms, authentication schemes are developed in [44], [122], [123], [124], [125], [126], [127], [128] and [129]. However, the transmission of the same unique pseudonym for each entity renders user tracking possible through network sniffing [130]. These challenges can be effectively addressed by the schemes in [131] and [132]. Unfortunately, the scheme in [132] cannot withstand privileged insider, impersonation, password guessing and man-in-the-middle attacks [133]. Additionally, it cannot offer perfect forward secrecy. Therefore, a lightweight authentication protocol is presented in [12].

To offer identity authentication, a novel scheme is developed in [134]. On the flip-side, this protocol cannot withstand user impersonation and privileged insider attacks [135]. Based on ECC, a mutual authentication protocol is introduced in [136]. Unfortunately, this scheme has extensive overheads that make it inefficient. This issue is resolved by the scheme in [137], which supports key exchange between the clients and cloud computing networks. It also protects against replay and man-in-the-middle attacks [138]. However, this scheme is defenseless against impersonation attacks [139]. On the other hand, an efficient biometric- based key agreement protocol is introduced in [140] for user authentication with the cloud infrastructure. Unfortunately, this technique has inefficient mutual authentication procedures. In addition, biometric-based authentication schemes are computationally inefficient when compared with legacy password-based authentication approaches. This is due to the extra computation costs incurred during biometric samples validation [141]. As such, the smart-card based scheme in [142] can be deployed. On the flip-side, this technique fails to provide user anonymity. Based on configurable PUF, a multi-factor mutual authentication protocol is introduced in [143]. Although the schemes in [144] and [145] offer some levels of security, they cannot withstand offline password guessing attacks. In addition, the approach in [144] cannot provide anonymity [146]. This problem is tackled by the dynamic pseudonym based authentication schemes in [147], [148], [149], [150], [151], [152], [153], [154], [155], [156], [157], [158], [159], [160], [161], [162] and [163]. As such, the eavesdropping the communication channel cannot yield any valid users identities [59], [164], [165]. Although tracking attacks are prevented, the verifier is able to map each authentication messages to a particular prover. In addition, the protocols in [154], [155], [157] and [163] involve some bilinear pairing operations, which are computationally extensive [166]. The elliptic curve point multiplication operations in [158], [159], [160], [161] and [162] also render these approaches computationally expensive. Therefore, the authors in [167] and [168] have proposed an energy-efficient and secure protocol. Unfortunately, the multi server cloud server authentication technique in [168] is vulnerable to man-in-the-middle attacks. It cannot also provide user anonymity. On the other hand, the RFID based mutual authentication protocol in [169] requires the execution of complex elliptic curve encryption. As such, it incurs high computing overheads [170], which is inefficient for the tags. This problem can be addressed by the multi-server environment security protocol in [171]. Unfortunately, this technique cannot withstand known temporary session key attacks.

To provide strong mutual authentication and key agreement, a secure protocol is presented in [1]. However, this technique is not resilient against password guessing attacks [172]. Additionally, its malicious user revocation mechanism is inefficient. To prevent adversaries from discerning the identities of clients from the network flow, security schemes have been developed in [147], [148], [149], [151], [152], [153], [154], [155], [158], [159], [160], [161], [162], [163]. However, the server is still capable of matching the authentication messages to a particular client identity or pseudonym. Therefore, truly anonymous algorithms have been presented in [59] and [165]. Whereas the approaches in [59] and [165] involve two parties, three parties are required in [58], including the TA. Unfortunately, the incorporation of the TA introduces some network bottlenecks.

Based on the above analysis, it is evident that strong security and privacy provision in the cloud environment still presents some challenges. For instance, the schemes in [32] and [36] share device identities openly over public channels. Coupled with their weak registration phase, this renders them susceptible to identity leakage and anonymity attacks. Similarly, the protocol in [173] is vulnerable to secret key disclosure, man in the middle and server impersonation attacks. Additionally, untraceability and anonymity cannot be upheld. It is also evident that while majority of these approaches support accountability, they can leak the private keys belonging to the cloud clients. In addition, many of these techniques incur heavy overheads during the authentication process [55]. Although three-factor authentication approaches are somehow more robust than two-factor schemes, they have some vulnerabilities. For instance, the ECC-based three-factor authentication technique in [174] is susceptible to known session key temporary, impersonation and privileged insider attacks. Regarding RFID-based authentication, threats such as packet replay, manipulation and interception are common on the communication channels [175]. In addition, unverified tags or readers can render the entire network untrustworthy. Moreover, these schemes have increased system overhead, which is not suitable for low-cost RFID tags [16]. Therefore, these methods cannot effectively offer balance between security and system overhead. Although the techniques in [176] and [177] can tackle this challenge, the approach in [177] cannot withstand known session temporary key and impersonation attacks.

3. Data sharing in the cloud techniques

The cloud repositories offer efficient management and convenient data access [118]. Cloud storage also offers efficiency and reliability. However, it also possess new challenges regarding personal data privacy and security. For instance, the exchange of the actual data over public clouds is a major security and privacy challenge to many enterprises and individuals. Therefore, numerous schemes have been put forward to address this critical challenge. For example, the authors in [Sultan et al., 2018] propose a reliable data distribution protocol. Although this method upholds controlled data access, it does not provide robust authentication to the legitimate clients before executing data operations. To this end, numerous machine learning algorithms [178] have been developed for threat detection [179], secure data sharing [180] and workload execution [181] over the cloud. Numerous symmetric encryption [182] and decryption algorithms have also been deployed by data delegators to boost convenience during data sharing [118]. To attain fast and early detection of distributed denial of service (DDoS) through HTTP flooding, a bio-inspired detection algorithm is developed in [179]. A protocol to facilitate secure data storage and controlled access over the cloud is presented in [183]. Unfortunately, arbitrary file transfer is not supported in this scheme. On the other hand, a machine learning based data sharing technique is developed in [180]. In this approach, data sharing decisions are made based on the granularity of requests, contextual and personal characteristics.

To offer convenient and flexible control to outsourced data, proxy encryption based access control protocols [184] are developed in [185], [186], [187], [188]. On the other hand, an android malware detection scheme is introduced in [189]. In this approach, mining of permission data is employed by machine learning classifiers [190] to classify various categories of benign and malicious applications. On their part, the authors in [191] have developed an access-controlled protocol for cloud storage based on symmetric cryptography. On the flip-side, user configuration is not supported by this method. Additionally, the protocols in [191] and [192] incur high communication and computation overheads during revocation. To facilitate user domain specific filtering, an ontology based classification [193] approach is introduced in [194]. This technique can therefore be incorporated to segregate legitimate cloud server login requests from spam or malicious ones. To facilitate a flexible configuration of data access on a deceptive storage server, an ECC based scheme is developed in [192]. This technique provides secure data transfers over the cloud environment. Unfortunately, during data re-encryption, the private key of the data delegator must be shared with the cloud storage. As such, these procedures violate secrecy and are inefficient [195]. To remedy this issue, authentication protocols security analysis scheme based on machine learning is developed in [196]. In Section 5, some guidelines and recommendations are elaborated that are thought to be crucial for the eradication or reduction of some of these challenges.

4. Results and discussion

In this section, the major findings are summarized in Table 1 and Table 2. Based on Table 1, it is clear that majority of the cloud computing security solutions have numerous merits and shortcomings. These challenges range from security, performance and privacy.

Table 1 Cloud computing security solutions

scheme	Pros	Cons
Kumar et al. [102]	Efficient and trustworthy	Stability challenges
Turkanovic et al. [134]	Provides user anonymity; can resist offline password- guessing attacks	Cannot resist privileged insider and user impersonation attacks
Kalra et al., [110]	Robust against replay, man in- the-middle, offline dictionary and cookie theft attacks	High computation overhead
Wu et al. [97]	Can resist temporary value disclosure and offline password guessing attacks	Not resistant against denial of service attacks; fails to offer perfect forward security
Kumar et al. [137]	Protects against replay & man-in-the-middle attacks	Defenseless against impersonation attacks
Tsai and Lo [119]	Can resist temporary value disclosure attacks; offers perfect forward security	Not resilient against server impersonation attacks
Gabsi et al.[169]	Protects tag privacy data	Huge computing overhead
Irshad et al. [73]	Resistant against user impersonation attacks; offers perfect forward security	Devoid of user registration and revocation phases
Sultan et al. [195]	Increased reliability; controlled data access	Does not provide robust authentication to the legitimate clients
Amin et al. [90]	Resilient against temporary value disclosure and privileged insider attacks	Not resistant against impersonation attacks
Martinez et al. [42]	Can resist user impersonation and offline password guessing attacks; offers user anonymity	Not resilient against session key disclosure attacks; cannot offer mutual authentication
Zhou et al. [44]	Offers user anonymity; resistant against privileged insider attacks; attains mutual authentication	Cannot resist packet replay, impersonation and temporary value disclosure attacks; fails to offer perfect forward security
Kang et al. [45]	Resilient against impersonation attacks; attains strong mutual authentication	Not resistant against offline password guessing attacks

In Table 2, a summary of the various security techniques and some of the schemes that employ them is given. As was the case for Table 1, these techniques introduce some challenges to the underlying security solutions.

Some of the most common techniques upon which most cloud computing security solutions are built include biometric, smart cards, blockchain, symmetric cryptography among others. In section 5, some recommendations are given on how some of these shortcomings can be addressed.

Table 2 Security techniques

Author	Technique	Cons
Sultan et al., [195]	Attribute-based	No authentication during data access
Kamara et al., [191]	Symmetric key	High communication and computation overheads No support for dynamic user configuration
Reddy et al., [142]	Smart-card	No support for user anonymity
Zhao et al., [192]	ECC	Insecure storage technique High execution overheads
Zhang et al. [67]	Blockchain	Inefficiency
Sun et al., [117]	ECC	No support for anonymity during authentication
Kumbhare et al., [183]	One-way hashing	No support for random file sharing
Das et al., [140]	Biometric	Sophisticated authentication procedures
Gope et al., [1]	Symmetric	Susceptible to offline password guessing attacks

5. Recommendations

The transmission of messages over public communication channels which is open and unprotected renders the cloud clients vulnerable to numerous attacks. Therefore, during data and services access, the users may face privacy data disclosure challenges. As such, the following precautions should be practiced during the client-cloud communication:

- Complete identity authentication must be executed every time the users want to access cloud services and data. This will facilitate the establishment of session keys to protect the data from possible tampering and disclosure.
- At present, QR codes and numerous authentications have been deployed for cloud computing security. However, it has been shown that these security techniques have various challenges such as susceptibility to man-in-the-middle and temporary value disclosure attacks. In addition, they have high complexities which are not ideal for resource limited IoT devices. Therefore, efforts should be dedicated to the development of lightweight security schemes to enhance efficiency and reduce energy consumptions.
- The public cloud is cheap and hence it reduces the costs of initial investment. Unfortunately, the public cloud lacks fie-grained security, control and optimum network settings. This can potentially discourage clients from deploying these cloud platforms. As such, security, performance and reliability should be considered at the design level of these cloud service models and communication protocols.
- In cloud storage, sufficient protection is required especially against privileged insiders. This calls for an authentication model for secure cloud storage access as shown in Figure 2. This will ensure that only legitimate users are allowed to register and utilize cloud data.
- As shown in Figure 2, user and cloud server registration takes place over secured channels. This ensures that attackers do not sniff the secrets being exchanged. After successful registration procedures, message exchanges among the user, control server and cloud server can be accomplished over public channels.
- Most of the legacy cloud systems use usernames and passwords for security. However, these two are ineffective in preventing data leakages in the cloud domain. There is therefore need for multi-factor, more secure and flexible systems for effective cloud data access.
- In the conventional cloud setup, there is one-to-one data distribution model. However, this model is inadequate especially for data originator control distribution model. As such, more parameters should be incorporated in data access systems to control the data delegator. These parameters need to facilitate the delivery of verifiable, correct, nontransferable and confidential data.
- In many cloud data distribution models, the data delegator assumes an active role in managing user accessibility and allows approved access to the stored data. Unfortunately, attribute and proxy-based

encryption may be inadequate for private cloud storage systems. This is attributed to data delegator ignorance of particular user's identity and preferences.

- Many organizations have turned to outsourcing data storage from the cloud. However, there have been numerous cyber attacks targeting different networks and cloud servers. This has led to privacy leakages that serve to impede the continued outsourcing activities. To curb this, there is need for strong entity authentication of all entities in this domain. These authentication procedures must be efficient, energy efficient and reliable.

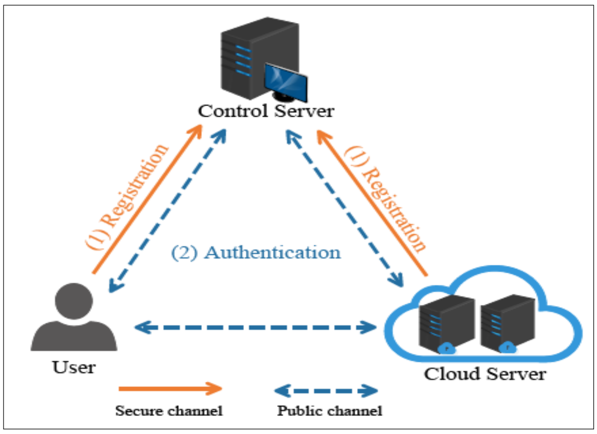

Figure 2 Cloud authentication model

- Owing to the popularity of public clouds, many business, organizations and corporations have deployed it for increased productivity. To access cloud services, numerous IoT devices are utilized. As such, there are massive volumes of data being exchanged over the public channels. In this environment, increased response latency and safe transmissions are key issues. These challenges can be overcome by the design of robust mutual authentication that incorporate strong cross-verification techniques.
- During private data transmission, numerous symmetric and asymmetric encryption techniques can be deployed. In symmetric encryption, the keys for encryption and decryption are exchanged between the client and the cloud. Such techniques include Advanced Encryption Standard (AES), RC5, Two- Fish, Data Encryption Standard (DES), RC6, 3DES and Blowfish. On the other hand, asymmetric encryption involves the usage of a pair of public and private keys in which the former is kept secret while the latter is publicly revealed. Some of these encryption algorithms include ECC and Rivest-Shamir-Adleman (RSA). Since symmetric encryption algorithms are more efficient than asymmetric algorithms, the former should be deployed in the cloud domain for reduced processing time and energy consumption

6. Conclusion

Many institutions and organizations have incorporated the cloud in their computing resource pools. The remote access of cloud data and services at any time and from any location on the globe has served to boost its adoption. However, the attack surface is always is increased when numerous devices connect to the cloud environment. In addition, a number of these connections take place over the open and unprotected public communication channels. Therefore, the cloud communication is characterized by numerous attacks and privacy violations. Consequently, many security solutions have been developed by various researchers to facilitate secure and efficient cloud data exchanges. However, the findings of this paper point to lack of sufficient protection of the stored data as well as the communication procedures. Towards the end of this paper, a number of recommendations have been highlighted. Future work will involve the practical implementation of these recommendations so that evaluations can be made and compared with the state of the art.

Compliance with ethical standards

Acknowledgments

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

References

[1] Gope P, Hwang T. An efficient mutual authentication and key agreement scheme preserving strong anonymity of the mobile user in global mobility networks. Journal of Network and Computer Applications. 2016 Feb 1;62:1-8.

[2] Botta A, De Donato W, Persico V, Pescapé A. Integration of cloud computing and internet of things: a survey. Future generation computer systems. 2016 Mar 1;56:684-700.

[3] Díaz M, Martín C, Rubio B. State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. Journal of Network and Computer applications. 2016 May 1;67:99-117.

[4] Sun P. Security and privacy protection in cloud computing: Discussions and challenges. Journal of Network and Computer Applications. 2020 Jun 15;160:102642.

[5] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan;13(2):691.

[6] Rashid A, Chaturvedi A. Cloud computing characteristics and services: a brief review. International Journal of Computer Sciences and Engineering. 2019 Feb;7(2):421-6.

[7] Shabaz M. A Secure Two-Factor Authentication Framework in Cloud Computing. Security and Communication Networks. 2022 Mar 12;2022.

[8] 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 Dec 1;23(4):145-62.

[9] Khan N, Zhang J, Ali J, Pathan MS, Chaudhry SA. A Provable Secure Cross-Verification Scheme for IoT Using Public Cloud Computing. Security and Communication Networks. 2022 Nov 23;2022.

[10] Nyangaresi VO, Ogundoyin SO. Certificate Based Authentication Scheme for Smart Homes. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 202-207). IEEE.

[11] Shen X, Gao J, Wu W, Li M, Zhou C, Zhuang W. Holistic network virtualization and pervasive network intelligence for 6G. IEEE Communications Surveys & Tutorials. 2021 Dec 15;24(1):1-30.

[12] Wu TY, Meng Q, Kumari S, Zhang P. Rotating behind Security: A Lightweight Authentication Protocol Based on IoT-Enabled Cloud Computing Environments. Sensors. 2022 May 19;22(10):3858.

[13] Hästbacka D, Halme J, Barna L, Hoikka H, Pettinen H, Larrañaga M, Björkbom M, Mesiä H, Jaatinen A, Elo M. Dynamic edge and cloud service integration for industrial iot and production monitoring applications of industrial cyber-physical systems. IEEE Transactions on Industrial Informatics. 2021 Apr 6;18(1):498-508.

[14] Shen X, Gao J, Wu W, Lyu K, Li M, Zhuang W, Li X, Rao J. AI-assisted network-slicing based next-generation wireless networks. IEEE Open Journal of Vehicular Technology. 2020 Jan 9;1:45-66.

[15] 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.

[16] Luo Y, Fan K, Wang X, Li H, Yang Y. RUAP: Random rearrangement block matrix-based ultra-lightweight RFID authentication protocol for end-edge-cloud collaborative environment. China Communications. 2022 Jul 22;19(7):197-213.

[17] Latha K, Sheela T. Block based data security and data distribution on multi cloud environment. Journal of Ambient Intelligence and Humanized Computing. 2019 Jul 20:1-7.

[18] Lim SY, Kiah MM, Ang TF. Security issues and future challenges of cloud service authentication. ActaPolytechnicaHungarica. 2017 Jan 1;14(2):69-89.

[19] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1;133:102763.

[20] Odelu V, Das AK, Kumari S, Huang X, Wazid M. Provably secure authenticated key agreement scheme for distributed mobile cloud computing services. Future Generation Computer Systems. 2017 Mar 1;68:74-88.

[21] Wang C, Ding K, Li B, Zhao Y, Xu G, Guo Y, Wang P. An enhanced user authentication protocol based on elliptic curve cryptosystem in cloud computing environment. Wireless Communications & Mobile Computing (Online). 2018;2018.

[22] Wu F, Li X, Xu L, Sangaiah AK, Rodrigues JJ. Authentication protocol for distributed cloud computing: An explanation of the security situations for Internet-of-Things-enabled devices. IEEE Consumer Electronics Magazine. 2018 Oct 5;7(6):38-44.

[23] 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.

[24] Bisht J, Vampugani VS. Load and Cost-Aware Min-Min Workflow Scheduling Algorithm for Heterogeneous Resources in Fog, Cloud, and Edge Scenarios. International Journal of Cloud Applications and Computing (IJCAC). 2022 Jan 1;12(1):1-20.

[25] Li W, Li X, Gao J, Wang H. Design of secure authenticated key management protocol for cloud computing environments. IEEE Transactions on Dependable and Secure Computing. 2019 Apr 9;18(3):1276-90.

[26] Li H, Yang C, Liu J. A novel security media cloud framework. Computers & Electrical Engineering. 2019 Mar 1;74:605-15.

[27] Joseph T, Kalaiselvan SA, Aswathy SU, Radhakrishnan R, Shamna AR. A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment. Journal of Ambient Intelligence and Humanized Computing. 2021 Jun;12(6):6141-9.

[28] 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.

[29] Singh AK, Saxena D. A cryptography and machine learning based authentication for secure data-sharing in federated cloud services environment. Journal of Applied Security Research. 2021 Jan 4:1-24.

[30] Saxena D, Vaisla KS, Rauthan MS. Abstract model of trusted and secure middleware framework for multi-cloud environment. InInternational Conference on Advanced Informatics for Computing Research 2018 Jul 14 (pp. 469-479). Springer, Singapore.

[31] Saxena D, Singh AK. Security embedded dynamic resource allocation model for cloud data centre. Electronics Letters. 2020 Sep;56(20):1062-5.

[32] Abbasinezhad-Mood D, Nikooghadam M. Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications. Future Generation Computer Systems. 2018 Jul 1;84:47-57.

[33] 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.

[34] Balaji NA, Sukumar R, Parvathy M. Enhanced dual authentication and key management scheme for data authentication in vehicular ad hoc network. Computers & Electrical Engineering. 2019 Jun 1;76:94-110.

[35] 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.

[36] Mahmood K, Chaudhry SA, Naqvi H, Kumari S, Li X, Sangaiah AK. An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. Future Generation Computer Systems. 2018 Apr 1;81:557-65.

[37] Ahmet F, Ferhat OM, Geoffrey CC. Password-based encryption approach for securing sensitive data. Security and Privacy. 2020:1-2.

[38] 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.

[39] Abdelfatah RI, Abdal-Ghafour NM, Nasr ME. Secure VANET Authentication Protocol (SVAP) Using Chebyshev Chaotic Maps for Emergency Conditions. IEEE Access. 2021 Dec 23;10:1096-115.

[40] Fan K, Zhu S, Zhang K, Li H, Yang Y. A lightweight authentication scheme for cloud-based RFID healthcare systems. IEEE Network. 2019 Mar 27;33(2):44-9.

[41] Pan JS, Sun XX, Chu SC, Abraham A, Yan B. Digital watermarking with improved SMS applied for QR code. Engineering Applications of Artificial Intelligence. 2021 Jan 1;97:104049.

[42] Martínez-Peláez R, Toral-Cruz H, Parra-Michel JR, García V, Mena LJ, Félix VG, Ochoa-Brust A. An enhanced lightweight IoT-based authentication scheme in cloud computing circumstances. Sensors. 2019 May 6;19(9):2098.

[43] 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.

[44] Zhou J, Cao Z, Qin Z, Dong X, Ren K. LPPA: Lightweight privacy-preserving authentication from efficient multi-key secure outsourced computation for location-based services in VANETs. IEEE Transactions on Information Forensics and Security. 2019 Jun 14;15:420-34.

[45] Kang B, Han Y, Qian K, Du J. Analysis and improvement on an authentication protocol for IoT-enabled devices in distributed cloud computing environment. Mathematical Problems in Engineering. 2020 Jun 23;2020.

[46] 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.

[47] Yu S, Park K, Park Y. A secure lightweight three-factor authentication scheme for IoT in cloud computing environment. Sensors. 2019 Aug 19;19(16):3598.

[48] Wang F, Xu G, Xu G, Wang Y, Peng J. A robust IoT-based three-factor authentication scheme for cloud computing resistant to session key exposure. Wireless Communications and Mobile Computing. 2020 Feb 18;2020.

[49] 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.

[50] Huang H, Lu S, Wu Z, Wei Q. An efficient authentication and key agreement protocol for IoT-enabled devices in distributed cloud computing architecture. EURASIP Journal on Wireless Communications and Networking. 2021 Dec;2021(1):1-21.

[51] Fan K, Luo Q, Li H, Yang Y. Cloud-based lightweight RFID mutual authentication protocol. In2017 IEEE Second International Conference on Data Science in Cyberspace (DSC) 2017 Jun 26 (pp. 333-338). IEEE.

[52] Wu F, Xu L, Kumari S, Li X, Das AK, Shen J. A lightweight and anonymous RFID tag authentication protocol with cloud assistance for e-healthcare applications. Journal of Ambient Intelligence and Humanized Computing. 2018 Aug;9(4):919-30.

[53] 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 Dec;11(4):66.

[54] Amin R, Islam SH, Kumar N, Choo KK. An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks. Journal of network and computer applications. 2018 Feb 15;104:133-44.

[55] Lyu Q, Li H, Deng Z, Wang J, Ren Y, Zheng N, Liu J, Liu H, Choo KK. A2UA: An Auditable Anonymous User Authentication Protocol Based on Blockchain for Cloud Services. IEEE Transactions on Cloud Computing. 2022 Oct 1(01):1-6.

[56] 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.

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

[58] Liu Y, Zhou T, Yue Z, Liu W, Han LY, Li Q, Yang X. Secure and Efficient Online Fingerprint Authentication Scheme Based on Cloud Computing. IEEE Transactions on Cloud Computing. 2021 Aug 10.

[59] Cassola A, Blass EO, Noubir G. Authenticating privately over public Wi-Fi hotspots. InProceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security 2015 Oct 12 (pp. 1346-1357).

[60] 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.

[61] Chandrakar P, Om H. An extended ECC-based anonymity-preserving 3-factor remote authentication scheme usable in TMIS. International Journal of Communication Systems. 2018 May 25;31(8):e3540.

[62] Mujahid U, Najam-ul-Islam M, Shami MA. RCIA: A new ultralightweight RFID authentication protocol using recursive hash. International Journal of Distributed Sensor Networks. 2015 Jan 26;11(1):642180.

[63] 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 Dec;39(10):e13126.

[64] Vijayakumar P, Obaidat MS, Azees M, Islam SH, Kumar N. Efficient and secure anonymous authentication with location privacy for IoT-based WBANs. IEEE Transactions on Industrial Informatics. 2019 Jun 26;16(4):2603-11.

[65] Yang Q, Xue K, Xu J, Wang J, Li F, Yu N. AnFRA: Anonymous and fast roaming authentication for space information network. IEEE Transactions on Information Forensics and Security. 2018 Jul 10;14(2):486-97.

[66] Wang Z, Fan J, Cheng L, An HZ, Zhang HB, Niu JX.. Supervised anonymous authentication scheme. Journal of software. 2019 Mar 28;30(6):1705-20.

[67] Zhang JY, Wang ZQ, Xu ZL, Ouyang Y, Yang T. A regulatable digital currency model based on blockchain. J. Comput. Res. Dev. 2018;55(10):127-40.

[68] 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.

[69] Cui J, Zhang X, Zhong H, Zhang J, Liu L. Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment. IEEE Transactions on Information Forensics and Security. 2019 Oct 11;15:1654-67.

[70] Lin C, He D, Huang X, Khan MK, Choo KK. DCAP: A secure and efficient decentralized conditional anonymous payment system based on blockchain. IEEE Transactions on Information Forensics and Security. 2020 Jan 27;15:2440-52.

[71] Yu P, Ni W, Yu G, Zhang H, Liu RP, Wen Q. Efficient anonymous data authentication for vehicular ad hoc networks. Security and Communication Networks. 2021 Feb 23;2021.

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

[73] Irshad A, Sher M, Ahmad HF, Alzahrani BA, Chaudhry SA, Kumar R. An improved multi-server authentication scheme for distributed mobile cloud computing services. KSII Transactions on Internet and Information Systems (TIIS). 2016;10(12):5529-52.

[74] Xiong L, Peng D, Peng T, Liang H. An enhanced privacy-aware authentication scheme for distributed mobile cloud computing services. KSII Transactions on Internet and Information Systems (TIIS). 2017;11(12):6169-87.

[75] Chien HY. SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. IEEE transactions on dependable and secure computing. 2007 Nov 12;4(4):337-40.

[76] 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.

[77] Bae WI, Kwak J. Smart card-based secure authentication protocol in multi-server IoT environment. Multimedia Tools and Applications. 2020 Jun;79(23):15793-811.

[78] Moon AH, Iqbal U, Bhat GM. Mutual entity authentication protocol based on ECDSA for WSN. Procedia Computer Science. 2016 Jan 1;89:187-92.

[79] Fakroon M, Alshahrani M, Gebali F, Traore I. Secure remote anonymous user authentication scheme for smart home environment. Internet of Things. 2020 Mar 1;9:100158.

[80] Banerjee S, Odelu V, Das AK, Chattopadhyay S, Park Y. An efficient, anonymous and robust authentication scheme for smart home environments. Sensors. 2020 Feb 22;20(4):1215.

[81] 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.

[82] Jia X, He D, Kumar N, Choo KK. A provably secure and efficient identity-based anonymous authentication scheme for mobile edge computing. IEEE Systems Journal. 2019 Feb 22;14(1):560-71.

[83] Chen CM, Huang Y, Wang KH, Kumari S, Wu ME. A secure authenticated and key exchange scheme for fog computing. Enterprise Information Systems. 2021 Oct 21;15(9):1200-15.

[84] Jia X, He D, Kumar N, Choo KK. Authenticated key agreement scheme for fog-driven IoT healthcare system. Wireless Networks. 2019 Nov;25(8):4737-50.

[85] 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.

[86] Ying B, Nayak A. Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public key cryptography. Journal of Network and Computer Applications. 2019 Apr 1;131:66-74.

[87] Doss R, Sundaresan S, Zhou W. A practical quadratic residues based scheme for authentication and privacy in mobile RFID systems. Ad Hoc Networks. 2013 Jan 1;11(1):383-96.

[88] Chiou SY, Chang SY. An enhanced authentication scheme in mobile RFID system. Ad Hoc Networks. 2018 Mar 15;71:1-3.

[89] 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.

[90] Amin R, Kumar N, Biswas GP, Iqbal R, Chang V. A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment. Future Generation Computer Systems. 2018 Jan 1;78:1005-19.

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

[92] Challa S, Das AK, Gope P, Kumar N, Wu F, Vasilakos AV. Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems. Future Generation Computer Systems. 2020 Jul 1;108:1267-86.

[93] Guo C, Luo N, Bhuiyan MZ, Jie Y, Chen Y, Feng B, Alam M. Key-aggregate authentication cryptosystem for data sharing in dynamic cloud storage. Future Generation Computer Systems. 2018 Jul 1;84:190-9.

[94] Karati A, Amin R, Islam SH, Choo KK. Provably secure and lightweight identity-based authenticated data sharing protocol for cyber-physical cloud environment. IEEE Transactions on Cloud Computing. 2018 May 8;9(1):318-30.

[95] Abood EW, Hussien ZA, Kawi HA, Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Kalafy A, Ahmad S. Provably secure and efficient audio compression based on compressive sensing. International Journal of Electrical & Computer Engineering (2088-8708). 2023 Feb 1;13(1).

[96] Djellalbia A, Badache N, Benmeziane S, Bensimessaoud S. Anonymous authentication scheme in e-Health Cloud environment. In2016 11th International Conference for Internet Technology and Secured Transactions (ICITST) 2016 Dec 5 (pp. 47-52). IEEE.

[97] Wu F, Li X, Xu L, Vijayakumar P, Kumar N. A novel three-factor authentication protocol for wireless sensor networks with IoT notion. IEEE Systems Journal. 2020 Apr 28;15(1):1120-9.

[98] Sadri MJ, Asaar MR. An anonymous two-factor authentication protocol for IoT-based applications. Computer Networks. 2021 Nov 9;199:108460.

[99] Nikooghadam M, Jahantigh R, Arshad H. A lightweight authentication and key agreement protocol preserving user anonymity. Multimedia Tools and Applications. 2017 Jun;76(11):13401-23.

[100] Fan K, Jiang W, Luo Q, Li H, Yang Y. Cloud-based RFID mutual authentication scheme for efficient privacy preserving in IoV. Journal of the Franklin Institute. 2021 Jan 1;358(1):193-209.

[101] 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.

[102] Kumar V, Kumar R, Jangirala S, Kumari S, Kumar S, Chen CM. An enhanced RFID-based authentication protocol using PUF for vehicular cloud computing. Security and Communication Networks. 2022 Jul 30;2022.

[103] Chatterjee U, Chakraborty RS, Mukhopadhyay D. A PUF-based secure communication protocol for IoT. ACM Transactions on Embedded Computing Systems (TECS). 2017 Apr 28;16(3):1-25.

[104] 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.

[105] Jiang Q, Zhang X, Zhang N, Tian Y, Ma X, Ma J. Three-factor authentication protocol using physical unclonable function for IoV. Computer Communications. 2021 May 1;173:45-55.

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

[107] Chen CT, Lee CC, Lin IC. Efficient and secure three-party mutual authentication key agreement protocol for WSNs in IoT environments. Plos one. 2020 Apr 30;15(4):e0232277.

[108] Hu B, Tang W, Xie Q. A Two-factor Security Authentication Scheme for Wireless Sensor Networks in IoT Environments. Neurocomputing. 2022 Jun 1.

[109] Kumar V, Mohanty S. A Secure Lightweight Mutually Authenticated Radio Frequency Identification (RFID) Protocol. In2018 5th International Conference on Signal Processing and Integrated Networks (SPIN) 2018 Feb 22 (pp. 914-918). IEEE.

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

[111] 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.

[112] 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.

[113] Luo M, Zhang Y, Khan MK, He D. A secure and efficient identity-based mutual authentication scheme with smart card using elliptic curve cryptography. International Journal of Communication Systems. 2017 Nov 10;30(16):e3333.

[114] Amin R, Maitra T, Giri D, Srivastava PD. Cryptanalysis and improvement of an RSA based remote user authentication scheme using smart card. Wireless Personal Communications. 2017 Oct;96(3):4629-59.

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

[116] Wang D, Mei Y, Ma CG, Cui ZS. Comments on an advanced dynamic ID-based authentication scheme for cloud computing. InInternational Conference on Web Information Systems and Mining 2012 Oct 26 (pp. 246-253). Springer, Berlin, Heidelberg.

[117] Sun H, Wen Q, Zhang H, Jin Z. A novel remote user authentication and key agreement scheme for mobile client-server environment. Applied Mathematics & Information Sciences. 2013 Jul 1;7(4):1365.

[118] Ghaffar Z, Shamshad S, Mahmood K, Obaidat MS, Kumari S, Khan MK. A Lightweight and Efficient Remote Data Authentication Protocol Over Cloud Storage Environment. IEEE Transactions on Network Science and Engineering. 2022 Sep 9;10(1):103-12.

[119] 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.

[120] 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.

[121] 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.

[122] Vijayakumar P, Azees M, Kozlov SA, Rodrigues JJ. An anonymous batch authentication and key exchange protocols for 6G enabled VANETs. IEEE Transactions on Intelligent Transportation Systems. 2021 Aug 4;23(2):1630-8.

[123] Vinoth R, Deborah LJ, Vijayakumar P, Gupta BB. An Anonymous Pre-Authentication and Post-Authentication Scheme Assisted by Cloud for Medical IoT Environments. IEEE Transactions on Network Science and Engineering. 2022 May 23.

[124] Lo NW, Tsai JL. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings. IEEE Transactions on Intelligent Transportation Systems. 2015 Dec 31;17(5):1319-28.

[125] Vijayakumar P, Chang V, Deborah LJ, Balusamy B, Shynu PG. Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks. Future generation computer systems. 2018 Jan 1;78:943-55.

[126] 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.

[127] 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.

[128] Zhang A, Lin X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. Journal of medical systems. 2018 Aug;42(8):1-8.

[129] Thwin TT, Vasupongayya S. Blockchain-based access control model to preserve privacy for personal health record systems. Security and Communication Networks. 2019 Jun 25;2019.

[130] 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.

[131] Kumar V, Ahmad M, Kumari A. A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS. Telematics and Informatics. 2019 May 1;38:100-17.

[132] Maitra T, Obaidat MS, Amin R, Islam SH, Chaudhry SA, Giri D. A robust ElGamal-based password-authentication protocol using smart card for client-server communication. International Journal of Communication Systems. 2017 Jul 25;30(11):e3242.

[133] 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.

[134] Turkanović M, Brumen B, Hölbl M. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. Ad Hoc Networks. 2014 Sep 1;20:96-112.

[135] 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.

[136] Kumari A, Jangirala S, Abbasi MY, Kumar V, Alam M. ESEAP: ECC based secure and efficient mutual authentication protocol using smart card. Journal of Information Security and Applications. 2020 Apr 1;51:102443.

[137] Kumar V, Ahmad M, Mishra D, Kumari S, Khan MK. RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing. Vehicular Communications. 2020 Apr 1;22:100213.

[138] 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.

[139] Safkhani M, Camara C, Peris-Lopez P, Bagheri N. RSEAP2: An enhanced version of RSEAP, an RFID based authentication protocol for vehicular cloud computing. Vehicular Communications. 2021 Apr 1;28:100311.

[140] Das AK. A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor. International Journal of Communication Systems. 2017 Jan 10;30(1):e2933.

[141] Nyangaresi VO. A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. Inthe 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation (605-612) 2021.

[142] Goutham Reddy A, Yoon EJ, Das AK, Yoo KY. Lightweight authentication with key-agreement protocol for mobile network environment using smart cards. IET Information Security. 2016 Sep;10(5):272-82.

[143] Melki R, Noura HN, Chehab A. Lightweight multi-factor mutual authentication protocol for IoT devices. International Journal of Information Security. 2020 Dec;19(6):679-94.

[144] Islam SH. Design and analysis of an improved smartcard-based remote user password authentication scheme. International Journal of Communication Systems. 2016 Jul 25;29(11):1708-19.

[145] Maitra T, Obaidat MS, Islam SH, Giri D, Amin R. Security analysis and design of an efficient ECC-based two-factor password authentication scheme. Security and Communication Networks. 2016 Nov 25;9(17):4166-81.

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

[147] Azees M, Vijayakumar P, Karuppiah M, Nayyar A. An efficient anonymous authentication and confidentiality preservation schemes for secure communications in wireless body area networks. Wireless Networks. 2021 Apr;27(3):2119-30.

[148] Zhou Y, Luo Y, Obaidat MS, Vijayakumar P, Wang X. PAMI-Anonymous Password Authentication Protocol for Medical Internet of Things. In2021 IEEE Global Communications Conference (GLOBECOM) 2021 Dec 7 (pp. 1-6). IEEE.

[149] 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.

[150] Nyangaresi VO, Abduljabbar ZA, Mutlaq KA, Hussain MA, Hussien ZA. Forward and Backward Key Secrecy Preservation Scheme for Medical Internet of Things. InHuman-Centric Smart Computing 2023 (pp. 15-29). Springer, Singapore.

[151] Aman MN, Basheer MH, Sikdar B. Data provenance for IoT with light weight authentication and privacy preservation. IEEE Internet of Things Journal. 2019 Sep 4;6(6):10441-57.

[152] Dawoud M, Altilar DT. HEADA: a low cost RFID authentication technique using homomorphic encryption for key generation. Security and Communication Networks. 2016 Nov 25;9(17):4182-91.

[153] 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.

[154] He D, Zeadally S, Kumar N, Wu W. Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures. IEEE transactions on information forensics and security. 2016 May 27;11(9):2052-64.

[155] Odelu V, Saha S, Prasath R, Sadineni L, Conti M, Jo M. Efficient privacy preserving device authentication in WBANs for industrial e-health applications. Computers & Security. 2019 Jun 1;83:300-12.

[156] 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.

[157] Arfaoui A, Boudia OR, Kribeche A, Senouci SM, Hamdi M. Context-aware access control and anonymous authentication in WBAN. Computers & Security. 2020 Jan 1;88:101496.

[158] Li X, Niu J, Bhuiyan MZ, Wu F, Karuppiah M, Kumari S. A robust ECC-based provable secure authentication protocol with privacy preserving for industrial internet of things. IEEE Transactions on Industrial Informatics. 2017 Nov 15;14(8):3599-609.

[159] 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.

[160] Shuai M, Yu N, Wang H, Xiong L. Anonymous authentication scheme for smart home environment with provable security. Computers & Security. 2019 Sep 1;86:132-46.

[161] Lyu Q, Zheng N, Liu H, Gao C, Chen S, Liu J. Remotely access "my" smart home in private: An anti-tracking authentication and key agreement scheme. IEEE Access. 2019 Mar 26;7:41835-51.

[162] Hammami H, Yahia SB, Obaidat MS. A lightweight anonymous authentication scheme for secure cloud computing services. The Journal of Supercomputing. 2021 Feb;77(2):1693-713.

[163] Maria A, Pandi V, Lazarus JD, Karuppiah M, Christo MS. BBAAS: Blockchain-based anonymous authentication scheme for providing secure communication in VANETs. Security and Communication Networks. 2021 Feb 18;2021.

[164] 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.

[165] Abdallah A, Shen XS. A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid. IEEE Transactions on Smart Grid. 2016 Apr 13;9(1):396-405.

[166] 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.

[167] Aghili SF, Mala H, Shojafar M, Peris-Lopez P. LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT. future generation computer systems. 2019 Jul 1;96:410-24.

[168] Kumari S, Li X, Wu F, Das AK, Choo KK, Shen J. Design of a provably secure biometrics-based multi-cloud-server authentication scheme. Future Generation Computer Systems. 2017 Mar 1;68:320-30.

[169] Gabsi S, Kortli Y, Beroulle V, Kieffer Y, Alasiry A, Hamdi B. Novel ECC-based RFID mutual authentication protocol for emerging IoT applications. IEEE Access. 2021 Sep 15;9:130895-913.

[170] 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.

[171] Feng Q, He D, Zeadally S, Wang H. Anonymous biometrics-based authentication scheme with key distribution for mobile multi-server environment. Future Generation Computer Systems. 2018 Jul 1;84:239-51.

[172] 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.

[173] Ali Z, Hussain S, Rehman RH, Munshi A, Liaqat M, Kumar N, Chaudhry SA. ITSSAKA-MS: An improved three-factor symmetric-key based secure AKA scheme for multi-server environments. IEEE Access. 2020 Jun 10;8:107993-8003.

[174] Ali R, Pal AK. An efficient three factor–based authentication scheme in multiserver environment using ECC. International Journal of Communication Systems. 2018 Mar 10;31(4):e3484.

[175] 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.

[176] Zhang J, Zhong H, Cui J, Tian M, Xu Y, Liu L. Edge computing-based privacy-preserving authentication framework and protocol for 5G-enabled vehicular networks. IEEE Transactions on Vehicular Technology. 2020 May 11;69(7):7940-54.

[177] Wang F, Xu G, Wang C, Peng J. A provably secure biometrics-based authentication scheme for multiserver environment. Security and Communication Networks. 2019 Jun 25;2019.

[178] Ghrabat MJ, Hussien ZA, Khalefa MS, Abduljabba ZA, Nyangaresi VO, Al Sibahee MA, Abood EW. Fully automated model on breast cancer classification using deep learning classifiers. Indonesian Journal of Electrical Engineering and Computer Science. 2022 Oct;28(1):183-91.

[179] Sreeram I, Vuppala VP. HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm. Applied computing and informatics. 2019 Jan 1;15(1):59-66.

[180] Bilogrevic I, Huguenin K, Agir B, Jadliwala M, Gazaki M, Hubaux JP. A machine-learning based approach to privacy-aware information-sharing in mobile social networks. Pervasive and Mobile Computing. 2016 Jan 1;25:125-42.

[181] Saxena D, Singh AK. A proactive autoscaling and energy-efficient VM allocation framework using online multi-resource neural network for cloud data center. Neurocomputing. 2021 Feb 22;426:248-64.

[182] 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.

[183] Kumbhare AG, Simmhan Y, Prasanna V. Designing a secure storage repository for sharing scientific datasets using public clouds. InProceedings of the second international workshop on Data intensive computing in the clouds 2011 Nov 14 (pp. 31-40).

[184] 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.

[185] Zhang J, Zhang Z. Secure and efficient data-sharing in clouds. Concurrency and Computation: Practice and Experience. 2015 Jun 10;27(8):2125-43.

[186] Li W, Xue K, Xue Y, Hong J. TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage. IEEE Transactions on parallel and distributed systems. 2015 Jun 22;27(5):1484-96.

[187] Chen Y, Song L, Yang G. Attribute-based access control for multi-authority systems with constant size ciphertext in cloud computing. China Communications Journal. 2016 Feb;13(2).

[188] Li Q, Ma J, Li R, Liu X, Xiong J, Chen D. Secure, efficient and revocable multi-authority access control system in cloud storage. Computers & Security. 2016 Jun 1;59:45-59.

[189] Li J, Sun L, Yan Q, Li Z, Srisa-An W, Ye H. Significant permission identification for machine-learning-based android malware detection. IEEE Transactions on Industrial Informatics. 2018 Jan 12;14(7):3216-25.

[190] Nyangaresi VO, El-Omari NK, Nyakina JN. Efficient Feature Selection and ML Algorithm for Accurate Diagnostics. Journal of Computer Science Research. 2022, 4(1): 10-19

[191] Kamara S, Lauter K. Cryptographic cloud storage. InInternational Conference on Financial Cryptography and Data Security 2010 Jan 25 (pp. 136-149). Springer, Berlin, Heidelberg.

[192] Zhao G, Rong C, Li J, Zhang F, Tang Y. Trusted data sharing over untrusted cloud storage providers. In2010 IEEE Second International Conference on Cloud Computing Technology and Science 2010 Nov 1 (pp. 97-103). IEEE Computer Society.

[193] Al Sibahee MA, Ma J, Nyangaresi VO, Abduljabbar ZA. Efficient Extreme Gradient Boosting Based Algorithm for QoS Optimization in Inter-Radio Access Technology Handoffs. In2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 2022 Jun 9 (pp. 1-6). IEEE.

[194] Rijvordt W, Hogenboom F, Frasincar F. Ontology-driven news classification with aethalides. Journal of Web Engineering. 2019 Nov 5:627-54.

[195] Sultan NH, Barbhuiya FA, Laurent M. ICAuth: A secure and scalable owner delegated inter-cloud authorization. Future Generation Computer Systems. 2018 Nov 1;88:319-32.

[196] Ma Z, Liu Y, Wang Z, Ge H, Zhao M. A machine learning-based scheme for the security analysis of authentication and key agreement protocols. Neural Computing and Applications. 2020 Nov;32(22):16819-31