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

Techniques and protocols for enhancing data privacy in cloud computing: A review

MARTIN OTIENO *

School of Informatics and Innovative Sciences, Jaramogi Oginga Odinga University of Science and Technology, Kenya.

World Journal of Advanced Engineering Technology and Sciences, 2023, 08(01), 391–404

Publication history: Received on 11 January 2023; revised on 25 February 2023; accepted on 27 February 2023

Article DOI: https://doi.org/10.30574/wjaets.2023.8.1.0064

Abstract

The emergence of cloud computing has enabled millions of devices across the globe to communicate and exchange massive amounts of data that is classified as private with each other. Given that these devices and platforms are scattered in different geographical areas, communicating with IoTs all the time, the issue of data security, in particular, assurance of data privacy has arisen. Several attempts in mitigating this issue has been by both academic and industry researchers in terms of technology, practices and protocols but it still remains a serious challenge even as cloud computing forges into the future. As a result, both individuals and organizations whose private data are held in the cloud are getting jittery due to the frequent data compromise or exposure in the cloud servers. This paper reviews the various challenges in data privacy and the mechanisms and techniques proposed by various researchers in bid to mitigate them and create a trustworthy cloud environment. It undertakes a comparative research analysis of the existing research work on data privacy protection techniques that have been proposed and implemented in the cloud computing environment.

Keywords: Cloud computing; Cloud security solutions; Privacy; Trust

1. Introduction

Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction [1], [2], [3], [4], [5]. According to NIST, cloud model is composed of five essential characteristics explained below:

On-demand self-services: broad network access; on-demand self-service; a consumer can unilaterally provision computing capabilities [6] such as server time and network storage as needed automatically without requiring human interaction with each service provider [7].

Broad network access: the capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations) [8], [9], [10], [11], [12].

Resource pooling: the provider's computing resources [13] are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand [14], [15]. This creates a sense of location independence since the customer generally has no control or knowledge over the exact location of the provided resources. The resources include storage, processing, memory and network bandwidth [16], [17], [18], [19], [20].

*Corresponding author: MARTIN OTIENO

Rapid elasticity: the capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand [21], [22], [23]. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service: the cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g. storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service [24], [25].

Cloud computing basically provides three service models including Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (SaaS) [26]. Software as a Service (SaaS) is the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure [27]. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings [28], [29]. Platform as a Service (PaaS) is the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming. Typically this is done on a pay-per-use or charge-per-use basis [30], [31], [32]. On the other hand, Infrastructure as a Service (IaaS) is the capability provided to the consumer for processing, storage, networks and other fundamental computing resources [33] where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components [34], [35].

Cloud computing also provides four deployment models including; private, public, community and hybrid cloud [36], [37]. In private cloud, the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed and operated by the organization or a third party and it may exist on or off premises [38]. Data owners have some control over their data, similar to intranets. Community cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy and compliance considerations) [39]. It may be owned, managed and operated by one or more of the organizations in the community or a third party and it may exist on or off premises. Control of data may be lost by the data owner in this model [7]. Public cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic or government organization and exists on the premises of the cloud provider. In this model, there is complete loss of control [40] by a user of their data.

Hybrid cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds) [7], [41], [42]. A cloud infrastructure consists of both physical layer and abstraction layer. The physical layer are the hardware resources that are necessary to support the cloud services being provided while the abstraction layer is the software deployed across the physical layer that manifest the essential cloud characteristics [43]. The abstraction layer sits above the physical layer implying that the user lacks control of the underlying cloud infrastructure including network, servers, operating systems and storage but only controls the deployed applications and configuration settings for the application-hosting environment [44]. In a bid to provide efficient services in these models, various challenges arise that impact negatively on data privacy [26].

Despite these challenges, Cloud computing has transformed the business and academic environments since its inception. Largely due to the internet environment that it thrives in, it has enabled organizations and individuals to off-load massive amounts of data from their own servers to off-shore storage servers [45]. It offers advantages and opportunities for business users to migrate and leverage the scalability of the pay-as-you-go price model [46]. It enables outsourcing information and business applications to the cloud or third parties. All these advantages are bedeviled with security and privacy concerns.

Cloud computing solves IT shortcomings such as poor utilization of resources, capacity planning, productivity, latency regarding application deployment and stagnant capabilities in optimizing and integrating an enterprise's IT stack [47]. IT functions are outsourced to service providers who manage the task and enable the enterprise to focus on its core functions and competencies to better drive its revenue and business model forward. It relieves firms and individuals of the costs of applications and platforms to conduct business and store data [48]. The process of outsourcing leads to loss

of data control by the cloud clients [49], [50]. Cloud providers would need to provide for increased regulation, certification, security, anonymity, trust by design and privacy by design in order to ease any concerns related to privacy and security [51] on the cloud.

NIST definition of cloud computing as enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources and their rapid provisioning and release with minimal management effort or service provider interaction imply loss of control by users of their data in the cloud. Users are concerned that the loss of control may enable the misuse of their data by cloud providers or compromise through hacker attacks on cloud data, a frequent occurrence in recent history. In 2014, hackers illegally accessed and exposed numerous celebrities' private photos stored on Apple's cloud service, iCloud. Recently, more than 200,000 CVs originating from two online recruiting firms were exposed after hacking attacks on their cloud storage service. Such data breaches highlight the importance of understanding the measures cloud providers have in place for data privacy and security [52], [53], [54], [55], [56], [57] before rushing into the cloud. Outsourcing information and business applications to third parties in cloud computing raises privacy concerns, a critical area in adopting cloud services. Entities that access cloud services almost always experience data security concerns as their networks are susceptible to vulnerabilities. These issues revolve mainly around authentication and social engineering and a lot of research in cloud computing security is currently focused here [58], [59].

As most business activities shift to online, cloud security issues continue to skyrocket. The ever-increasing activities of malicious criminals highlight many cloud flaws including; remote access, end-user education and awareness especially, against social engineering , mis-configured cloud systems, BYOD policies, social engineering attacks such as phishing, phishing with malware payloads and brute force attacks and Distributed Denial-of-Service (DDoS) [58], [60], [61].

Criminals exploit the increase in cloud use, targeting mainly, private data from healthcare facilities, financial, governance and other online critical services and they are far more proactive than the cyber security teams. Human error is one area of concern for organizations as it is the weakest and most exploited by criminals. This is mainly on authentication and social engineering issues, an area that many researchers in cloud computing security tend to focus on. Endpoint user error or negligence requires continuous training and education in an effort to prevent criminals who continually, increase their efforts to tap into such holes in cloud architecture [62], [63]. The same end users would be the most concerned about privacy/confidentiality [64] of their data .However, most privacy research in the cloud domain focuses on technical solutions and rarely mention the cloud service users' privacy concerns [65], [66].

2. Paper contributions

- This paper surveys research works on cloud security in the area of data privacy in order to unearth some weaknesses associated with the security protocols and techniques that have been developed and adopted by the authors.
- It offers an insight into the workings of these designs and how they can be hardened in order to enhance data privacy in the cloud.

3. Benefits of Cloud computing

The following have been cited as the main benefits for the deployment of cloud computing in any organization:

- Scalability: this is the cloud services' ability to scale as per business needs, an invaluable attribute as it relieves an organization from investment in IT infrastructure resources and software applications as all are provided by a cloud services vendor [67], [68], [69]. Scalability [70] occurs in two ways; increasing user licenses during business booms or enhancing application software to cater to a growing business [71].
- Low Cost: this is because the cloud services allow customers to access cloud storage, application software, and backup facilities without the need to invest in IT hardware and software infrastructure that supports these services and also does away with the need for hardware maintenance and software upgrades. Instead, users pay an annual or monthly subscription to cloud service providers to access these services [72]. Essentially cloud services convert capital expenditure to operating costs [71].
- Enhanced Flexibility: Organizations enjoy the flexibility to use cloud services when in need only, which reduces costs and at the same time provides assurance of processing capacity [73] to meet demand. If additional resources are no longer needed, organizations can cancel the cloud service subscription [71].
- High Processing Speeds: Cloud service users experience an efficient data system that is not plagued by congestion, network unreliability, breach threats or common inefficiencies of most on-premises systems [74],

[75]. Cloud services use advanced algorithms [76] which optimize servers and find the most efficient routes to guide data traffic [71].

- Data Security: Cloud services are obliged to use the latest and most efficient data security measures [77], [78], [79], due to the large quantity of data handled through their cloud systems. Security of customer data is a prerequisite, as well as being a daily function. Hence, cloud services use security systems [80], [81], [82], [83] that utilize a distributed architecture that can absorb, filter, and deflect malicious requests that pose a threat to the system [61], [71].

These benefits have made many organizations to leverage onto cloud services, improving their overall efficiency by focusing on key business objectives as the cloud providers handle their data issues including data security [84]. Manpower is freed to engage in other tasks, creating economic value. However, their reliance on the cloud providers for data security and lack of control over their data in the cloud creates a security and data privacy problem as they do not know where the data is stored or even how it is handled at the storage location [61], [85].

The authors in [86] contend that cloud providers must guard against theft or denial-of-service attacks by users against other users and providers against users as the provider controls the "bottom layer" of the software stack, effectively circumventing most known security techniques [87], [88], [89]. They do this through virtualization security, a defense mechanism that protects against most attempts by users to attack one another or the underlying cloud infrastructure. They also contend that not all resources are virtualized and not all virtualization environments are bug-free, implying that virtualized code may "break loose" to some extent [86]. Incorrect network virtualization can also allow user code access to sensitive portions of the provider's infrastructure, or to the resources of other users. There is also the risk of inadvertent data loss and all this impact heavily on users' data privacy in the cloud [90].

Researchers in cloud computing security are majorly concerned with managing accessibility, authentication controls against the backgrounds of costs in terms of energy consumption and communication versus efficiency [91], [92], [93]. They have developed protocols, algorithms and techniques to try and balance these requirements. Most of these controls are usually too costly but efficient or cheap but may not mitigate threats. Some of the security approaches in the literature to tackle the present security flaws lack the flexibility in mitigating multiple threats without conflicting with cloud security objectives [94].

4. Schemes for data security and privacy protection

American Psychology Association (APA) defines privacy as 'the right to control (psychologically and physically) others' access to one's personal world (APA Dictionary), such as by regulating others' input through use of physical or other barriers (e.g., doors, partitions) and by regulating one's own output in communication with others; to control the amount and disposition of the information one divulges about oneself [85].

Informational privacy is "a state or condition of controlled access to personal information" [95]. It is infringed whenever another party has access to one's personal information by reading, listening, or using any of the other senses [95]. It is the exposure of the "virtual person" to unauthorized "eyes". Privacy and informational privacy may not be fixed as it is rare for anyone to permanently remain in a condition of complete physical or informational inaccessibility to others [96], [97]. The existence of informational privacy rights implies the duty of cloud providers either not to disclose information or to prevent unauthorized access to information by others [98]. Information privacy is the right to have control over how one's personal information is collected and used and cloud providers are expected to adhere to this [85]. However, with advance in technological innovation, information privacy has become more and more complex as more data is collected and exchanged and technology gets more invasive. The cloud computing providers may be unaware of the fact that they are processing personal data, which [99] refer to as the "cloud of unknowing". The multi-layered structure of cloud computing services creates issues in relation to the correct identification of the data controller and processor and the consequent allocation of responsibilities.

As a consequence, cloud providers face an incredibly complex risk matrix for ensuring that personal information is protected and therefore, privacy has fast-emerged as the most significant consumer protection issue in the cloud technology. Figure 1 below shows the framework of cloud security with the key principles of data security including data privacy [100]. Data privacy, as seen in the figure, apart from being one of the key principles of data security, connects the cloud infrastructure with other key principles. Its importance can therefore, not be ignored when developing or implementing any data security mechanism, policy or protocol.

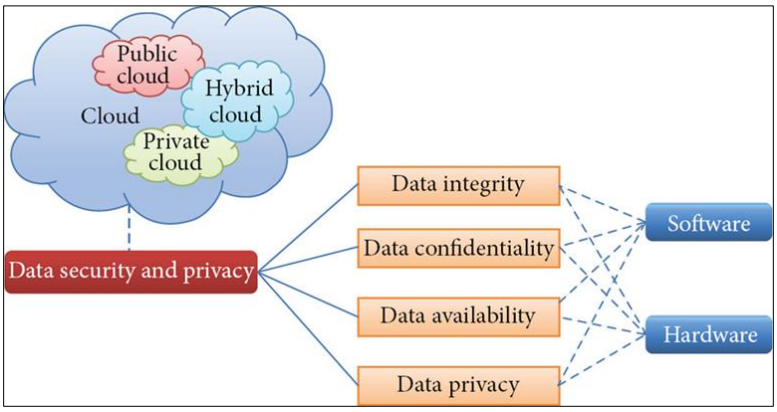

Figure 1 Cloud service security framework [85], [95], [99]

5. Research Findings

While data security rotates around the three key principles; confidentiality, integrity and availability, the survey found out most of the protocols and techniques presented focused on protection of data confidentiality by eliminating vulnerabilities in data transmission and message communication. Some of the works emphasize on the strength of symmetric encryption algorithm in combined with other techniques and protocols. The reviewed literature agrees with the Figure 1 placement of data privacy and recognizes it as a significant issue in cloud security. They further propose its enforcement using strong authentication mechanisms. Data encryption schemes and other cryptographic techniques [101] such as EC-cryptography, use of combinations such as blockchain and encryption to harden cloud servers were proposed by the authors. The following table represents some of the proposed solutions to issues of data privacy by some researchers. We review their strengths and weaknesses in enforcing data privacy in cloud computing architecture in this paper.

The authors in [59] have proposed an authentication protocol based on a symmetric encryption algorithm and fog computing in the Internet of Vehicles. The use of SGX, a security software that only includes hardware thus avoiding software vulnerabilities and malicious threats in the system, largely ensures system security enhances confidentiality, hence, privacy of vehicle data. It also proposes to provide a trusted execution environment inaccessible to malicious code, guaranteeing data confidentiality and integrity. The authors in [60] argue that the use of EC cryptography hardened the encryption schemes that were used in combination with it. It improves the assurance of confidentiality through anonymity, where the identities of the client and the cloud servers are hidden from everyone [60], [102], [94]. [60] in their proposed cloud security model, tackles the problem of privacy by use of EC cryptographic technique for both patient and doctor anonymity, together with message authentication but the patient has no way of being assured that their private medical data is protected. The protocol lacks patient feedback mechanism.

The authors in [103] identify Confidentiality, Integrity and Availability as the challenging issues associated with data storage management in data outsourcing. According to the illustration of cloud service security framework in Figure 1 above, they equally recognize data privacy as significant. They propose a method of data storage which achieves CIA using data dispersal whose practicality is demonstrated by implementing it in a private cloud setup using the OpenStack cloud framework. However, they are unable to demonstrate its success neither in public cloud nor in implementation of data privacy [104]. Neither does it have a feedback nor is an assurance mechanism for users to know if their private data is really private. The fact that providers also deny users control over their data leads to questions over privacy of data, especially when the provider folds up or ownership is transferred.

Data replication in different servers across geographical regions to ensure no downtime to users also raised question of privacy. The authors in [105] observe that the traditional data encryption has always been used to secure such data. They further emphasize that a system that employs encryption for data outsourcing is secure if it ensures correctness, confidentiality and data access privacy. They further emphasize that a system that employs encryption for data outsourcing is secure if it ensures correctness, confidentiality and data access privacy. However, the failure of traditional encryption schemes has seen development of new techniques as seen in table above that attempt to solve the problem. [60] also demonstrate that their work, RAPCHI is not vulnerable to replay and man-in-the-middle attacks and therefore can assure data privacy of patients who are the users. The question that begs is that it doesn't give a feedback on that assurance and the patient may lack a basis to trust the technique. Trust is generally defined as a willingness to accept vulnerability based on positive expectations of another party [95], with two critical elements; the psychological state of

willingness to be vulnerable and positive expectations of another party. The patients' expectations of the technique would thus be lowered and pose questions on the state of their private data.

The authors in [60] make use of One-way hash function with strong-collision resistance where if $h(x) = h(y)$ is the output, then finding pair (x, y) with $x \neq y$ then is computationally impossible to ensure integrity of user (doctor and patient) passwords which provides assurance to users their passwords cannot be cracked hence data is safe. However, repeated use of one-way hash functions weakens their security, hence easily compromised. They could strengthen the use of one way hash function by salting them; addition of cryptographically secure random string to the passwords before hashing it. The authors in [106] argue that although hashes play important role in ensuring data privacy and security, their algorithms may have some loopholes that are exploitable. The combination scheme between password and salt is therefore, enables the hardening of the security of one way hash algorithms. Salted hashing is a much more complex and secure process because each hash requires the use of a different and random 'salt', that acts as an additional layer of encryption. Since the salt is not stored with the hash, attackers typically cannot determine which hashing scheme was used and therefore cannot reverse engineer the hash [106]. Other approaches have integrated cryptography and machine learning approaches to provide multiple security features against DOS attack, impersonation attack, phishing attack, replay attack, ID and password leakage attack [107], [108]. They posit that the protocol safe from many possible security attacks occur during online data sharing under multi-cloud environment.

In their work, the authors in [109] agree with [60] on their use of ECC arguing that it uses with smaller keys to provide high security and high speed in a low bandwidth. The authors in [110] also support use of ECC in cloud security. They posit that ECC reduces energy consumption and maximizes devices' efficiency by using small crypto keys with the same strength of the required cryptography of other cryptosystems and is thus, the preferred approach for many environments including the Internet of Things (IoT) and wireless sensor networks (WSNs), some key technologies supporting cloud computing. A major implementation issue of ECC is associated with private key management. It is required to ensure that the private keys are being re-calculated and re-issued regularly as constant usage of private keys seriously increases the risk of keys being intercepted by a third party. This further weakens [60] technique on cloud data privacy.

The authors in [102] proposed a one way hash and nonce-based two-factor secure authentication scheme with traditional user IDs, password, and OTP verification procedure that could resist brute force attack, session and account hijacking attack, MITM attacks, and replay attacks. They leverage on the superiority of Elliptic Curve Cryptography (ECC) over Rivest-Shamir-Adleman (RSA) encryption scheme in terms of speed and security obtainable by an ECC that allows faster execution and a superior user experience. They too support the efficiency and lightweight-ness of ECC over other encryption schemes.

The authors in [111] have proposed data security with elliptic curve cryptography, a proficient data security model algorithm, as a secure tool to model a secured platform for data in cloud computing. However, it has been found that Elliptic curve-based cryptosystems usually suffer implementation issues associated with insufficient software testing and computer system security audits including technical errors in hardware and software implementations in the form of lack of authentication, inadequate RAM and media protection and errors in algorithms among others [112]. This may lead to sensitive information, including private encryption getting into the hands of third parties without them having to break the cryptosystem's fundamental security background and instead, accessing the data directly through the hardware and software security holes. ECC also suffers implementations problems associated with private key management as it is required to ensure that the private keys are re-calculated and re-issued regularly. Usage of constant private keys increases the risk of keys being intercepted by a third party.

Authors in [58] assert that secure mutual authentication is an indispensable requirement to share organizational invaluable data among collaborating entities in federated cloud environment. They propose a mutual authentication method that incorporates machine learning based ensemble Voting Classifier for online threat detection and Elliptic Curve Cryptography with Schnorr's signature scheme based key agreement to ensure secure communication by prior detection and mitigation of security breaches. The approach proposes an efficient and lightweight approach for authentication of participating entities as it blocks malicious entity from accessing the shared data. Like the previous authors in [60] and [102] base their proposed scheme on elliptic curve cryptography (ECC) for its superior security and scalability with low communication and computation costs.

The authors in [113] in their work on CKMIB: Construction of Key Agreement Protocol for Cloud Medical Infrastructure Using Blockchain assert that storing all electronic healthcare data in blockchain as proposed by other researchers is too difficult because to the price and size of block chain. They proposed a new key agreement and authentication protocol for cloud medical system using blockchain that is secure in security attacks such as impersonation, eavesdropping,

stolen verifier, insider assault, replay and man in the middle attacks. They also use hash function that has the weakness that was described in [60] above.

Authors in [61] in their work 'Security of Zero Trust Networks in Cloud Computing: A Comparative Review.' observe that despite the network shift from traditional in-house servers to third-party-managed cloud platforms for cost-effectiveness and increased accessibility, these networks remains reactive and relatively un-accountable for its overall data security. They review the zero-trust network architecture (ZTNA), an emerging technology approach to the security of cloud networks where no entity is implicitly trusted in the network, regardless of its origin or scope of access. ZTNA proactively predicts threats based on users' behaviour. ZTNA should enable network administrators to tackle critical issues on how to inhibit internal and external cyber threats, enhance the visibility of the network, automate the calculation of trust for network entities and enhance security for users. They discussed challenges associated with requirements for migrating to zero-trust architecture and the possible future research directions where new technologies can be incorporated into the ZTA to build robust trust-based enterprise networks deployed in the cloud.

The authors in [114] propose a ultra-lightweight encryption function and proposes an RFID authentication scheme based on this function for the end-edge-cloud collaborative environment. This ultra-lightweight RFID mutual authentication protocol is based realizes the mutual authentication of readers, tags and edge servers in insecure communication channels and realizes the balance between security and system costs. The findings from the review of the techniques and protocols proposed by the various authors are summarized in the Table 1 below.

Table 1 Current security schemes

Author	**Solution offered**
Tsu-Yang et al. [59]	Provided an authentication protocol based on a symmetric encryption algorithm and fog computing in the Internet of Vehicles.
Wu et al. [115]	Presented an Intel software-guard-extensions (SGX)-based authentication key agreement protocol in an IoT-enabled cloud computing environment.
Luo et al. [114]	Presented Random Rearrangement Block Matrix-Based Ultra-Lightweight RFID Authentication Protocol for End-Edge-Cloud Collaborative Environment
Wu et al. [116]	Presented a Lightweight Authentication Protocol Based on IoT-Enabled Cloud Computing Environments
Singh and Saxena [58]	Presented a Cryptography and Machine Learning Based Authentication for Secure Data-Sharing in Federated Cloud Services Environment
Shabaz et al., [102]	Presented Secure Two-Factor Authentication Framework in Cloud Computing
Ghaffar et al. [36]	Presented a Lightweight and Efficient Remote Data Authentication Protocol Over Cloud Storage Environment
Abdulsalam et al. [94]	Reviewed different works in the literature, "Security and Privacy in Cloud Computing: Technical Review.", their adaptiveness in mitigating against future reoccurring threats and showed how cloud security conflicts have invalidated their proposed models.
Kumar et al. [117]	Presented a Provably Secure ECC and Biometric Based Authentication Framework Using Smartphone for Vehicular Cloud Environment
Kumar et al. [60]	RAPCHI; presented a robust technique to protect cloud medical data from MIM, confidentiality, repudiation and anonymity.
Sarkar et al. [61]	Security of Zero Trust Networks in Cloud Computing: A Comparative Review
Itoo et al. [113]	CKMIB: Construction of Key Agreement Protocol for Cloud Medical Infrastructure Using Blockchain

The study looked at the handling of three aspects of data security in the reviewed papers. The three aspects included data confidentiality, privacy and trust, the areas cloud users are highly concerned about [106], [109], [118]. Lack of assurance on data privacy could lead to trust issues in data security techniques proposed.

In the "data everywhere" world that organizations operate in today, controlling who or what has access to information is essential for securing it. The reviewed works all had various forms of identity and access management (IAM) with user identities and access, captured and recorded, an assurance that they can verify, authenticate, authorize and audit all individuals and services properly. Most of the reviewed techniques gave a holistic approach to privacy and by approaching it from different layer, from hardware to applications. Most of the reviewed work did not focus on the area of data privacy alongside trust assurance in their proposed models. These findings are illustrated in Table 2 below.

Table 2 Data security areas of confidentiality, privacy and trust

Author	Data confidentiality	Data privacy assurance	Trust assurance
Kumar et al. [60]	√	X	X
Kumar et al. [117]	X	X	X
Ghaffar et al. [36]	√	X	X
Shabaz et al. [55]	√	X	X
Itoo et al. [113]	√	X	X
Khan et al. [118]	X	X	X
Sarkar et al. [61]	√	X	X
Shabaz et al. [102]	√	X	X
Singh et al. [58]	√	X	X
Wu et al. [59]	√	X	X
Wu et al. [115]	√	X	X
Wu et al. [116]	√	X	X
Luo et al. [114]	√	X	X

From the analysis of the works of the researchers above, this review found out that although they proposed very strong authentication protocols and techniques that could resist many security attacks, there still exist many loopholes that may not provide assurance of data privacy to users. The research proposes embedding other techniques such as salting of hashes, use of pseudonymisation among others to enhance data privacy. Salting passwords before hashing would reinforce the encryption scheme as it would be technically difficult to find the correct hash value by an attacker. Pseudonymisation of private data is a technique associated with the EU's General Data Protection Regulation (GDPR) to protect personal data. Pseudonymisation refers to techniques that replace, remove or transform information that identifies individuals and keep it separate such that the data does not point at any identifiable entity while remaining personal in scope of data protection law. This would reduce the risks posed during data processing, data for archiving, scientific and historical research. It is distinct from anonymity that most of the authors proposed as anonymous information is information, not related to any identified or identifiable individual, thus not subject to regulations while pseudonymised data remains personal data,

This paper also suggests combination of technologies for both perimeter and internal data security for cloud services to ensure privacy. An example proposed in [119], where Zero-Trust, used to validate transactions and nodes with varying levels of Trust can be combined and used with other novel technologies such as blockchain and the IoT. As authors in [61] explains, there are currently many technologies developed for specific areas of data security and unfortunately, none provide a comprehensive platform or a 'one-size-fits-all' type of system. As a result, this review proposes that more research be undertaken in this important area of cloud security that impacts heavily on trust of cloud services.

6. Conclusion

This study found out that, despite efforts to improve cloud data security, many researchers do not focus to what remains valuable to cloud users; the privacy of their data. The study therefore recommends that Cloud service providers embed Privacy policies in cloud security services that are flexible and responsive to the users' needs while enhancing data privacy. It also recommends further research on enhancement of the users having full control in choosing privacy preferences for their data with capability of monitoring it. Further research should be done to develop techniques that enable cloud users to be able to evaluate the security posture of cloud vendors before sharing their confidential or sensitive data. The security for data portability across different platforms should be further enhanced using appropriate security protocols and standards. To assure users of data privacy, since the user has very little control over movement of their data, cloud providers can implement pseudonymisation of data to protect personal data.

Compliance with ethical standards

Acknowledgments

I would like to extend my appreciation to all my family members and colleagues who offered a helping hand during the development of this manuscript.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Feb 8:103117.

[7] Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. A view of cloud computing. Communications of the ACM. 2010 Apr 1, 53(4):50-8.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] Zhang Q, Cheng L, Boutaba R. Cloud computing: state-of-the-art and research challenges. Journal of internet services and applications. 2010 May, 1:7-18.

[25] 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.

[26] Sun Y, Zhang J, Xiong Y, Zhu G. Data security and privacy in cloud computing. International Journal of Distributed Sensor Networks. 2014 Jul 16, 10(7):190903.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

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

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

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Jul 9, 3(5):364.

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

[47] Murphy B, Rocchi M. Ethics and Cloud Computing. Data Privacy and Trust in Cloud Computing: Building trust in the cloud through assurance and accountability. 2021:105-28.

[48] 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).

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

[50] 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).

[51] 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.

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

[53] 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.

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

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

[56] 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.

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

[58] 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. 2022 Jul 3, 17(3):385-412.

[59] Wu TY, Guo X, Chen YC, Kumari S, Chen CM. Sgxap: Sgx-based authentication protocol in iov-enabled fog computing. Symmetry. 2022 Jul 6, 14(7):1393.

[60] Kumar V, Mahmoud MS, Alkhayyat A, Srinivas J, Ahmad M, Kumari A. RAPCHI: Robust authentication protocol for IoMT-based cloud-healthcare infrastructure. The Journal of Supercomputing. 2022 Sep, 78(14):16167-96.

[61] Sarkar S, Choudhary G, Shandilya SK, Hussain A, Kim H. Security of zero trust networks in cloud computing: A comparative review. Sustainability. 2022 Sep 7, 14(18):11213.

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

[63] 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.

[64] 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.

[65] Jain P, Gyanchandani M, Khare N. Big data privacy: a technological perspective and review. Journal of Big Data. 2016 Dec, 3:1-25.

[66] Nikkhah HR, Grover V, Sabherwal R. Why do users continue to use mobile cloud computing applications? A security-privacy.

[67] 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.

[68] 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.

[69] 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.

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

[71] Kuo TW, Liou BH, Lin KC, Tsai MJ. Deploying chains of virtual network functions: On the relation between link and server usage. IEEE/ACM Transactions On Networking. 2018 Jun 20, 26(4):1562-76.

[72] 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.

[73] 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.

[74] 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.

[75] 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.

[76] Nyangaresi VO, El-Omari NK, Nyakina JN. Efficient Feature Selection and ML Algorithm for Accurate Diagnostics. Journal of Computer Science Research. 2022 Jan 4, 4(1):10-9.

[77] 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.

[78] 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.

[79] 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.

[80] 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.

[81] 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.

[82] 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.

[83] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. InEmerging Technologies in Computing: 4th EAI/IAER International Conference, iCETiC 2021, Virtual Event, August 18–19, 2021, Proceedings 4 2021 (pp. 3-20). Springer International Publishing.

[84] 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.

[85] Peras D, Mekovec R. A conceptualization of the privacy concerns of cloud users. Information & Computer Security. 2022 Apr 12.

[86] 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.

[87] 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.

[88] 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.

[89] 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.

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

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

[92] 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.

[93] 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.

[94] Abdulsalam YS, Hedabou M. Security and privacy in cloud computing: technical review. Future Internet. 2022 Jan, 14(1):11.

[95] Schwartz PM. Information privacy in the cloud. U. Pa. L. Rev.. 2012, 161:1623.

[96] 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.

[97] 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.

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

[99] Hon WK, Millard C, Walden I. The problem of 'personal data'in cloud computing: what information is regulated?—the cloud of unknowing. International Data Privacy Law. 2011 Nov 1, 1(4):211-28.

[100] 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.

[101] 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.

[102] Shabaz M. A secure two-factor Authentication framework in cloud computing. Security and Communication Networks. 2022 Mar 12, 2022.

[103] Tchernykh A, Schwiegelsohn U, Talbi EG, Babenko M. Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. Journal of Computational Science. 2019 Sep 1, 36:100581.

[104] 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.

[105] Sion R. Secure Data Outsourcing. InVLDB 2007 Sep 23 (Vol. 7, pp. 1431-1432).

[106] Sugiantoro B. Analysis of Password and Salt Combination Scheme To Improve Hash Algorithm Security. International Journal of Advanced Computer Science and Applications. 2019, 10(11).

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

[108] 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.

[109] Paul S, Krishna A, Qian W, Karam R, Bhunia S. MAHA: An energy-efficient malleable hardware accelerator for data-intensive applications. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. 2014 Sep 4, 23(6):1005-16.

[110] Almajed H, Almogren A, Alabdulkareem M. iTrust—A Trustworthy and Efficient Mapping Scheme in Elliptic Curve Cryptography. Sensors. 2020 Nov 30, 20(23):6841.

[111] 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.

[112] 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.

[113] Itoo S, Khan AA, Kumar V, Alkhayyat A, Ahmad M, Srinivas J. CKMIB: Construction of key agreement protocol for cloud medical infrastructure using blockchain. IEEE Access. 2022 Jun 21, 10:67787-801.

[114] 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.

[115] Wu TY, Wang L, Guo X, Chen YC, Chu SC. SAKAP: SGX-Based Authentication Key Agreement Protocol in IoT-Enabled Cloud Computing. Sustainability. 2022 Sep 5, 14(17):11054.

[116] 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.

[117] Kumar V, Kumar R, Kumar V, Kumari A, Kumari S. RAVCC: Robust Authentication Protocol for RFID based Vehicular Cloud Computing. J. Netw. Intell. 2022, 7:526-43.

[118] Khan IA, Qazi R. Data security in cloud computing using elliptic curve cryptography. International Journal of Computing and Communication Networks. 2019 Aug 27, 1(1):46-52.

[119] Dhar S, Bose I. Securing IoT devices using zero trust and blockchain. Journal of Organizational Computing and Electronic Commerce. 2021 Jan 2, 31(1):18-34.