Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 180 - 192
Received 16 February 2021; Accepted 08 March 2021.

A Study on Security Services and Threats in Cloud Computing

S. Vidyasagar[1], Dr.A.Murugan[2]
[1]Department of Computer Science and Engineering,SRMIST,Kattankulathur, India.
[2]Department of Computer Science and Engineering, SRMIST, Kattankulathur, India.

ABSTRACT
Cloud computing revolutionises many environments with the easy-to-use, easy to-connect, customise, automate and flexible services available to enterprises. This transition in mindset raises the need to take into account a wide variety of security and privacy concerns. In the cloud computing world, multi-tenancy, lack of control and morale are main problems. This paper discusses the latest developments and a broad variety of recent and innovative cloud protection and private privacy initiatives. In addition to the analysis of current advances in the security of confidentiality of sensitive data, such as privacy-based vulnerability modelling and privacy enhancement protocols, we categorise previous research based on cloud-related infrastructure, service regulation, and cloud service management layers.

KEYWORDS
Cloud Computing, Trend Analysis, Graphical Interpretation.

Introduction

Many of our ecosystems, including wellness, are revolutionised by cloud computing. Cloud computing environments, in contrast to earlier processes in data management, offer essential advantages, such as the provision of automatic assembly, connection, setup, and on-demand configuration resources. These promote the accomplishment of corporate priorities because cloud services can be accessed by companies effectively. Nevertheless a paradigm change that goes hand and hand that leads to security and privacy aspects such as multi-tenance, faith, lack of power, and accountability[1]. As a result, cloud systems managing confidential information must incorporate technological and operational protections to prevent breakdowns in data security which could result in massive and expensive damages. Sensitive cloud computing knowledge contains information from a multitude of disciplines and sectors. Health data is a common example of the confidential information managed in cloud systems, and it is clear that most people expect health information to be secure. As these new cloud systems have proliferated in recent years, the standards in privacy and data security have changed, shielding people from monitoring and database exposure. The EU Data Security Directive[2] and the United States Health Insurance Portability and Transparency Act (HIPAA) are some examples for such defensive legislation[3], all of which require protection of privacy for personal information handling. This article offers an analysis of security and privacy studies in cloud environments in sensitive data. We find emerging innovations in the cloud provider's levels of orchestration, management of infrastructure, physical devices and cloud services. In order to manage confidential data such as the simulation of privacy vulnerability and the improvement of privacy protocols and solutions, we also investigate the new privacy strategy.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 180 - 192
Received 16 February 2021; Accepted 08 March 2021.

Theoretical Background

Cloud infrastructure has proven promising and best adapted for the online management of data and software. Its use is restricted because of data protection. Cloud platforms are rendered more reliable with any computing or solutions [3].

In compliance with our report, the highest volume of paperwork is based on cloud storage protection providers. Data storage security, network security, time reduction, cost reduction, intrusion safety, like DOS and DDoS threats.

Many researchers have demonstrated their attempts to enhance the previously explained limits by suggesting various protocols, algorithms, error-bound solutions, defining or demonstrating the work focused on maximizing efficiency.

A. Security in Data Storage

Recently, cloud infrastructure is the most widely used technologies. There are more free clouds available to enable clients to save their information in the cloud storage. Users and businesses can require important and costly cloud storage details. The encryption or decryption method for cloud data storage protection [4].

B. Personal Security in Network

Using OpenStack Network Virtualization Technology concept, the commonly accepted open-source application that can implement the IaaS model of cloud-based infrastructure. OpenStack allows the cloud manager to organize the hosting cluster and handle the computing facilities [4].

C. Personal Security and Privacy

Service providers guarantee that any confidential information is disguised or shielded, the details can be viewed by authorised customers only. Furthermore, the digital identification and credential as should other details the provider receives or generates regarding the customer's actions.

D. Reduce Time and Reduce Cost

In order to help a broad variety of real-life applications including Industrial Automation as a cloud technology for automation systems design [6], new cloud technologies are being created.

Security Approach through Existing Technologies

While cloud storage provides several benefits, there are still many significant hurdles to adoption. Protection, following compliance concerns, privacy and legal issues, is the primary reason for barriers to adoption [7]. Since cloud computing is a modern concept, the manner in which different level of security provided (e.g., network, host, system, data level), application protection may be transferred to cloud computing is quite confusing [8, 9]. This uncertainty has repeatedly prompted knowledge managers to claim that protection is their first priority for cloud computing [10]. This portion deals with existing cloud protection models, methods and algorithms. The

literature review is discussed.

Gonzales, D. et al presents the Cloud-Trust Protection Evaluation Concept for Infrastructure as a Service (IaaS) clouds [11]. It is a cloud infrastructure guide model that incorporates a broad variety of security measures and standard practise, as well as a cloud security appraisal model (Cloud-Trust), which calculates high-level security metrics in order to decide the level of secrecy. Two problems for the IaaS are discussed with respect to the optimised fine-grained and fair price scheme [11]: (1) services manufacturers and customers' earnings are always mutually contradictory; (2) overheads for VM maintenance including start-up costs are often too high to overlook.

Biometric encryption [12] is suggested to enhance cloud storage confidentiality for biometric details. The privacy of a specific individual applies to biometric details, i.e. facial data for well-known and influential individuals. This paper also discussed cloud storage virtualization and biometrics encryption.

No Central Authorities and no secure set-up are required under the Decentralized multi-authority attribute-based signature (DMA-ABS) scheme[13].The provide a wide class (non-monotons) predicate is entirely secure under the traditional consideration of linear (DLIN) decision-making in a oracle process. Outsourced ABS[14] lowers the overhead on the customer side dramatically by outsourcing intense processing through an untrusted Cloud Signature Service (S-CSP).

Multi-factor authentication (MFA) [15] is a validation process which involves two or more authentication factors. Since cloud services are popular, MFA systems are becoming important for authenticating users. The privacy security multi-factor authentication framework, which incorporates large-scale data features named MACA[15]. In this, initial process is password, while the other factor is the hybrid user activity profile.

Homomorphic encryption is a method of encryption enabling the measurement of cypher material, thereby creating an encrypted outcome that matches the results of plaintext operations when it is decrypted; it allows the computation of encrypted data to be conveniently computed, and it also enables encrypted details to be computed without decryption. Additionally, the homomorphic properties of the different cryptosystems will also help to many protected structures, such as safe voting systems [17], collision-resistant hash functions, private recovery schemes and much more. Craig Gentry[18] identified the very first feasible creation utilising grid-based cryptography of a completely homomorphic encryption system.
The ID-based cloud storage user authentication[19] framework facilitates higher protection and lower computing costs. In [20], Cloud Storage service is implemented by authentication scheme. It provides privacy and simplicity for smartphone consumers to use a single private key to access various service providers' mobile cloud storage facilities. The proposed scheme is based on the bilinear combination of the encryption mechanism and the complex nonce generation. Improved Security Improved Authentication for Remote Users and cloud storage Key Arrangement [21]. It helps the consumer and the cloud server to anonymously authenticate each other and to establish a protected channel between them. Thus, the communication transmitted can only be known through the receiver and the cloud service. None but themselves can learn about the true identity of the message sender.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 180 - 192
Received 16 February 2021; Accepted 08 March 2021.

A modern mutual authentication technique [22] is proposed under which the consumer and cloud service may authenticate. The protocol is configured to use steganography as an alternative coding scheme. The scheme is authenticated using hidden exchange. Secret exchange enables confidentiality to be maintained on both ends, which, when mixed, becomes a secret. The secret requires details regarding the two individuals concerned. Band authentication has also been utilised, adding more security. The suggested protocol includes the session key between the users and cloud service to be exchanged. Users were also offered the option of modifying their passwords.

A. Schemes ABE

Fuzzy Identity-Based Encryption [23] has been proposed Attribute Dependent Encryption (ABE). Identity is used function as a collection of descriptive qualities. In IBE, the user can decrypt the ciphertext, only if there is same identity. Fuzzy IBE will decrypt the message if the identity overlaps surpass the reset threshold between the sender and the receiver. The consumer will have number of attributes in ABE, additionally with identity. The KP-ABE method and the CP-ABE scheme is separated as two groups.

B. KP-ABE Scheme

The sender has an entry policy for data encryption in the main policy ABE or KP-ABE (Goyal et al., [24]). Cipher-text is identified from the category of attributes, that's lies as part of cipher-text encryption policy. Author represents the attributes and keys are deleted cannot write down any stallion content. The user collects attributes and hidden keys from the attribute authority and may decrypt knowledge.

Unfortunately, since the access policy is designed into a hidden key, the KP-ABE device data owner is unable to decide who will decode the cipher text and choose the collection of attributes to monitor the cipher text access. The method of access often includes a single-handed access mechanism, which cannot bear a negative attribute excluding those that do not wish to share data with the data holders. Subsequently, Ostrovsky et al., [25] suggested a non-monotronic access scheme where hidden keys provide a range of attributes of positive and negative attributes. This framework increase the ciphertext size and the hidden key while still adding overhead encryption and decryption. Lewko et al. [26] recently improved its original build, leveraging a modern technology to achieve consumer revoking and creation of the most successful non-monotronic KP-ABE scheme. KP-ABE schemes, In this methodology, the ciphertext size is incremented in line with the amount of cypher text attributes and limited forms of threshold access policy are a recognized exception.

C. CP-ABE Scheme

In 2007, Bethen court et al., suggested the first construction of the CP-ABE utilising the monotone control tree as an access structure[27]. Their framework follows adaptive access management policies like the KP-ABE [8] method in accordance with general group paradigm. Cheung and Newport [28] have allows a validated and secure CP-ABE system that is validated as stable by the mainstream model and supports AND as its access policy a key to positive and negative attributes[29]. He conveyed access control through the Linear Secret Sharing Scheme

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 180 - 192
Received 16 February 2021; Accepted 08 March 2021.

(LSSS) across the attributes in the framework (frameworks are momentarily expressed by LSSS). The text size of cipher, the overhead ciphertext process rises linearly with the difficulty of the access formula in this most successful scheme. In the end, Lewko et al., [30] have recently used the Waters coding technique [29] to build a Water Encoding scheme to achieve adaptive (non-selective) security. The method is therefore as effective and practical as Bethencourt et al., [27]. Their structures are based on the compound order groups, resulting in a lack of versatility relative to water. Emura et al., [31] improved competitiveness and adopted a covert agenda.

D. Dual-Policy ABE Scheme

A new ABE system called the Dual-policy ABE scheme was implemented by Attrapadung and Imai[32] in 2009. It is actually a mixed Goyal et al system. Scheme KP-ABE[33] scheme Waters CP-ABE[29]. It requires simultaneous access through encrypted data to control mechanisms. These two access management systems allow for only one of the above functions at a time. In addition, protection proof is based on the decision-making statement provided by the Diffie-Hellman exponent (DBDHE).

E. MA-ABE Scheme

There may be two classes with multiple ABE schematics[34, 35]. One needs a central authority (CA) who can also decode any encrypted letter, like schemes [34, 36], while other wants no CA like schemes [37**,** 38]. The other does not need a CA. [38].By, &, we signify the number of universal attributes, user U attributes and cypher text attributes. The IU and IC are the authority's index collection. By E and P, one paring operation is described as exponential. By LG1 and LG2, we mean that the number of authorities inside the systems is one aspect of Group G1 and that of Group G2 respectively.

F. Attribute-Based Proxy Re-encryption Scheme

Proxy recryption (PRE) is advised to improve the efficiency of data sharing. The Public Key Encryption (PKE) is to enable the transition of decryption rights is extended by PRE, implemented by Mambo and Okamoto. It allows a buddy named a proxy to transform an encrypted cypher text in owner’s public key to another ciphertext in the same plain text for user. But neither decoding key nor the plaintext underlying it is known by the proxy.

G. HABE Scheme

Hierarchical attribute-based encryption systems (HABE) by the combination of the hierarchical HIBEsystem and the cipher text-policy-based attribute encryption framework (CP-ABE) to provide not only fine grained access controls.

This scheme used key properties for producing keys in the HIBE method. Furthermore, disjoints standard (DNF) type was employed to communicate access control protocol, which included five functions: the cloud storage supplier, the data controller, the root authority, the data user and the data authority managed by the same domain authority.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 180 - 192
Received 16 February 2021; Accepted 08 March 2021.

Present study is concentrated through the nature of cloud access management. With the exception of all other schemes, ABE encryption is included in attributes. One of the primary economic benefits of the new encryption systems is that decryption is costly for resource-limited machines due to combination activity and the amount of pairing operations needed to decode the ciphertext increasing with the sophistication of the access policy. The system uses a symmetrical key method and no authentication process. These current structures are mostly centrally offered and do not support several readings or writings. The authors, however, have a standardised means of spreading secret keys and attributes to all users in a single key distribution centre (KDC). Another important issue for the current infrastructure is continuous data sharing and connectivity. The most significant requirement in the cloud is message secrecy authentication.

Literature Survey

The rewards of cloud storage are not retrieved through this scheme which trigger cloud users discomfort. The problem of key revocation in this work would therefore be addressed with a recent protection principle called revocable identity-based broadcasting proxy re-encryption (RIB-BPRE). In the sense of RIB-BPRE, a proxy may delete a number of delegates from the re-encoding key allocated by the Delegator[34].

IDPP [35] suggests a mechanism to secure sensitive protection for identity-based broadcast proxy re-encryption (RBP). (RBP) Proxy Re-encryption [35]. P2B uses the Lagrange theorem of interpolation to send the identities of a broadcast re-encrypted chiphertexte recipient party privacy. Proxy re-encryption is an easy solution for safe cloud data exchange with recipients. The sender has to regenerate the re-encryption key for each recipient to exchange data with a community of recipients, which contributes to an overall on the sender hand. To address the issue, identification-based proxy re-encoding is extendable to identity-based re-encoding of broadcast proxies.

The keyword search based on attributes[36] focuses on a particular and difficult situation in which the data collection can be searchable by several owners and can be searched by many users. We suggest an attribute-driven keyword check with effective revocation scheme (AKSER) based upon our research into ABE (Attribute Base Encryption). Our method is incredibly effective with regard to user revocation and allows for fine-grained search approval from the distributed permitted institution for the various attributes.

A stable and expandable vehicle network authentication schema[37] that satisfies the ever-expanding, diversified consumer service needs. Our approach allows the vehicle to only register once with the Trustworthy Authority (TA) to ensure easy and effective authentication of the vehicles using CSPs. Further the new CSP can engage in vehicle operation as long as it is successfully registered in TA. A TA-managed cloud broker links all cloud providers, and thus masks the difficulties involved in choosing CSPs from the view of the customer. A thorough safety review has demonstrated that our scheme will satisfy conditional security of privacy and achieve vehicle network safety objectives.

Stable attribute-based data sharing[38] tackles this problem with a modern, resource-limited mobile device cloud-based data-sharing scheme. By incorporating public device parameters, the proposed scheme reduces a significant number of the calculation tasks in addition to partially

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 180 - 192
Received 16 February 2021; Accepted 08 March 2021.

transferring offline encryption. In addition, before the decryption process a public ciphertext test phase is conducted to remove most overhead computations owing to unlawful ciphertexts. A chameleon hash function is used for data protection in order to produce immediate ciphertext, which is blinded to the final online ciphertexts by the oflineciphertexts. The suggested arrangement has been shown to be protected from adaptively selected assaults, generally accepted as a default notion of protection.

A protocol focused on blockchain shared authentication and a key smart grid agreement [39]. In specific, through blockchain leverage the protocol will enable successful confidentiality and key control without the need for other sophisticated rudimentary cryptographs. A proven dynamic reverse three-factor MAK A protocol that allows user dynamic management utilisingSchnorr signatures and offers a structured protection proof for the random oracle, is provided inside the Stable Authenticated Key Management Protocol [40]. Security research reveals that in multi-server contexts, our protocol will satisfy different needs.

Online/offline keyword encryption [41] provides an online/offline keyword search system (OOABKS) for mobile cloud. In order to minimise online prices and local measurement costs for smartphone devices, we use ABE online and offline and use ABE technologies. And we are enforcing the user's fine grain access regulation. Security research reveals that trapdoor connectivity, keyword safety, data protection security and search control are feasible with our scheme.

A new notion of proxy-re-encryption (PBRE) transmitted proxy [42]. In a PBRE method, Alice will assign the right to decryption to a community of users at a certain time, thereby enabling the re-encryption of Alice's cypher code. We propose a PBRE method and demonstrate its security in a random oracle assumption against a chosen-ciphertext attack (CCA). Dynamic fog-changing [43] should be clear to fog consumers with a data security authentication scheme. Our approach is to create a shared authentication between Fog users at the network edge and the Fog layer servers. In order for fog user-fog server to authenticate and set up a session key without revealing the actual user identity, we suggest a reciprocal authentication scheme that is anonymous. We use Pseudonym Based Cryptography PBC, Elliptic Curve Discrete ECDLP and Bilinear Pairing to evaluate the session key.

The signature on identity[44] is an anonymous main Smart Grid technology partnership protocol. This procedure helps the smart metres to use the utilities they offer anonymously with the energy power. In the absence of trustworthy authorities, the intelligent metres understand this goal with a private key. Only after registration is the trusting authority concerned. A random oracle model and ProVerification automated method test and validate the suggested procedure.

This provides [45] a modern anonymous broadcast encryption (A 2 B 2 E) which includes secret access policy property and enables the data owner to interact his/her data with multiple participants in the preset receiver and comply with the access policy. In addition to the detailed and systematic protection facts without the help of the randscape models, we first propose a particular A 2 B 2 E method. Then via the A 2 B 2 E, verifiable external decryption technologies for attribute-based crypting and the concept of the online/offline attribute-based script, we are building an effective and stable data-sharing framework.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 180 - 192
Received 16 February 2021; Accepted 08 March 2021.

The key concern is that when uploaded the consumer loses complete power. During machine architecture, this dilemma needs to be tackled. This essay analyses many computer management methods and strategies maintained on the cloud and the concealment of confidential and private data. The paper further addresses the different challenges facing the usage or use of the techniques. A scheme is introduced here, utilising cryptography, algorithms and secure cloud storage [46]. Here a system is proposed.

CP-ABE Schemes [47] enable data owner, before outsourcing to the Cloud, to encrypt data in the desired access framework. The encrypted data can only be deciphered by those that have a validated attribute collection matching the Access framework. Despite benefits comparison with standard encryption algorithms, CP-ABE schemes remain difficult to withdraw attributes and users. Firstly, current revocation methods cannot address the issue thoroughly since they create protection vulnerabilities and raise device overhead. Secondly, forward security is not specifically taken into consideration of which withdrawn people cannot decipher details that they have exchanged in the past. We analyse these problems in this paper and establish two CP-ABE systems, which permit both productive users and revoking attributes. Inclusion of re-encryption methods guarantees the potential secrecy provision for the planned systems.

A one-to-many data exchange scheme to solve this issue is safe and verifiable [48]. We use blockchain to log access policies and do not repudiate the customer and the cloud. We suggest an appropriate qualification scheme in light of the computing skills of the car consumers. In the meantime, we suggest a policy hiding scheme in terms of the classified details used in the access policy.

E-Vote-as-a-Service [49] focused onimplementing a recently designed and adaptable electronic voting service using blockchain technology. The aim is to create anarchitecture to convert the client defined service configuration into a cloud-based deployable package, automation of business logic specification, blockchain configuration, and cloud service provider selection. The article points out the preliminary findings of the method and the SOA-based description of services is implied.

ChainSplitter [50] designed an architecture fora hierarchical storage infrastructure, most of the blockchain is stored in the cloud storage. The blocks are stored in the IIOT network on overlay network for it.This work combines on local IIOt network, blockchain overlay network, cloud infrastructure,blockchain and cloud connector, hierarchical blockchain storage. The blockchain connector helps to construct each block in blockchain created in IIOT networks, and the cloud connector helps to label the synchronization issues.

ChainFS[51] a middleware framework that secures cloud storage services utilizing a trusted Blockchain. ChainFS hardens cloud storage protection against forking attacks. ChainFS middleware open file system interface to clients. ChainFS manages data in the cloud and transfer limited and required functionality to the Blockchain for the main district. This implement the ChainFS system onEthereum, S3FS and closely integrate it with FUSE clients andAmazon S3 cloud storage.

Privacy preservation [52] proposed the architecture of a new identity and access management system as part of FaaS, a cloud federation service developed by the H2020 SUNFISH project.

This framework helps federated entities to implement attribute-based access control plans on their data in a privacy-preserving manner. Users are given access to federated data when their identity attributes similar to the plans, but without disclosing their attributes in a consistent manner.

A Privacy-Preserving Voting Protocol on Blockchain[53] is the fundamental concept of decentralization of blockchain and exposes the fraud. To enable decision-making in a decentralized and safe manner, proposed a native blockchain voting protocol for peers to vote on their current blockchain network without the need for other one. Our protocol protects the anonymity of the end-to-end and possesses valuable properties such as detectability and correctability. Related implementation of Hyperledger Fabric protocol, which demonstrates the validity and functional application of this protocol, is also given.

Conclusion

This work surveyed the current developments in security and privacy research in cloud storage services. It defined a range of key cloud computing principles and technologies, such as virtualization, and containers. This also focused on wide range of security issues posed by current or potential privacy legislation, such as the EU DPD and the HIPAA. The findings in the field of cloud security and privacy are focused on activities of cloud providers, such as orchestration, abstraction, physical resource and cloud service management layers. Data security considerations influencing the actions of cloud providers in regards to the legitimate processing of customer data have been established and a study of existing studies has been undertaken to review the state-of-the-art in the area.

References

[1]A Vouk, Mladel. “Cloud computing- Issues, Research and Implementation”. CIT. *Journal of Computing and Information technology 16.4*(2008):235-246.

[2]Uddin, Shahadat, et al. "Trend and efficiency analysis of co-authorship network." *Scientometrics* 90.2 (2011): 687-699.

[3]Bapat, Devavrat, et al. “A Cloud Computing Security Solution Based on Fully Homomorphic Encryption.”

[4]S.M. Metev and V. P. Veiko, “*Laser Assisted Microtechnology*”, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

[5]V Callegati, Franco, et al. “Performance of Network Virtualization in cloud computing infrastructures: The OpenStack case.” *Cloud Networking (CloudNet), 2014 IEEE 3rd International Conference on. IEEE*, 2014.

[6]Hegazy, Tamir, and Mohamed Hefeeda. “Industrial automation as a cloud service.” *Parallel and Distributed Systems, IEEE Transactions on* 26.10 (2015): 2750- 2763.

[7]Ju KPMG (2010) from hype to future: KPMG’s 2010 Cloud Computing survey. http://www.techrepublic.com/whitepapers/from-hype-to-future-kpmgs-2010-cloud-computing-survey/2384291.

[8]ShyamNandan Kumar, “DecenCrypto Cloud: Decentralized Cryptography Technique for Secure Communication over the Clouds.” *Journal of Computer Sciences and Applications,*

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 180 - 192
Received 16 February 2021; Accepted 08 March 2021.

vol. 3, no. 3 (2015): 73-78.

[9] Rosado DG, Gómez R, Mellado D, Fernández-Medina E (2012) Security analysis in the migration to cloud environments. *Future Internet 4*(2):469-487.

[10] Mather T, Kumaraswamy S, Latif S (2009) *Cloud Security and Privacy*. O'Reilly Media, Inc., Sebastopol, CA.

[11] Hai Jin, Xinhou Wang, Song Wu and Sheng Di, "Towards Optimized Fine-Grained Pricing of IaaS Cloud Platform", *IEEE Transactions on Cloud Computing*. Vol 3, issue 4, pp. 436-448, (2015).

[12] Omar, M.N, Salleh, M., and Bakhtiari, M., "Biometric encryption to enhance confidentiality in Cloud computing", *International Symposium on Biometrics and Security Technologies (ISBAST), 2014, IEEE*, 45-50, Kuala Lumpur.

[13] Tatsuaki Okamoto and Katsuyuki Takashima, "Decentralized Attribute-Based Signatures", *Public-Key Cryptography – PKC 2013, Springer Berlin Heidelberg*, pp 125-142.

[14] Xiaofeng Chen, Jin Li, Xinyi Huang, Jingwei Li, Yang Xiang and Duncan S. Wong, "Secure Outsourced Attribute-Based Signatures", pp: 3285-3294, IEEE, vol. 25, (2014).

[15] Wenyi Liu, Uluagac, A.S. and Beyah, R., "MACA: A privacy-preserving multi-factor cloud authentication system utilizing big data", *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2014, pp. 518-523, Toronto, ON.

[16] Craig Gentry, *A FULLY HOMOMORPHIC ENCRYPTION SCHEME",* PhD Thesis, STANFORD UNIVERSITY, September 2009.

[17] Ron Rivest (2002-10-29). "Lecture Notes 15: Voting, Homomorphic Encryption.

[18] Craig Gentry, "Fully Homomorphic Encryption Using Ideal Lattices", ACM 978-1-60558-506-2/09/05, STOC'09, May 31–June 2, 2009, Bethesda, Maryland, USA.

[19] Jen Ho Yang and Pei Yu Lin, "An ID-Based User Authentication Scheme for Cloud Computing", *Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, 2014, IEEE, pp. 98-101, Kitakyushu.

[20] Jia-Lun Tsai and Nai-Wei Lo, "A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services", *Systems Journal, IEEE* (Volume: 9, Issue: 3), pp. 805-815, 21 May 2015.

[21] Zheming Dong, Lei Zhang and Jiangtao Li, "Security Enhanced Anonymous Remote User Authentication and Key Agreement for Cloud Computing", *IEEE 17th International Conference on Computational Science and Engineering (CSE),* 2014, pp. 1746-1751, Chengdu.

[22] Nimmy, K., and Sethumadhavan, M., "Novel mutual authentication protocol for cloud computing using secret sharing and steganography*", Fifth International Conference on the Applications of Digital Information and Web Technologies (ICADIWT), 2014, IEEE*, pp. 101-106, Bangalore.

[23] A. Sahai and B. Waters, "Fuzzy identity-based encryption", *In EUROCRYPT, ser. Lecture Notes in Computer Science*, vol. 3494. Springer, pp. 457-473, 2005.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 180 - 192
Received 16 February 2021; Accepted 08 March 2021.

[24] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data," *in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06). ACM*, 2006, pp. 89-98.

[25] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," *In Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07),* 195-203, November 2007.

[26] A. Lewko, A. Sanais, and B. Waters, "Revocation systems with very small private keys," *In Proceedings of the IEEE Symposium on Security and Privacy (SP '10),* pp. 273-285, Oakland, Calif, USA, May 2010.

[27] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," *in Proceedings of the IEEE Symposium on Security and Privacy (SP '07),* pp. 321-334, May 2007.

[28] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," *in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07),* pp. 456–465, November 2007.

[29] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," *In Public Key Cryptography (PKC '11),* pp. 53-70, Springer, Berlin, Germany, 2011.

[30] A. Lewko, T. Okamoto, A. Sahai, and B. Waters, "Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption," *In Advances in Cryptology: EUROCRYPT* 2010, vol. 6110 of Lecture Notes in Computer Science, pp. 62-91, Springer, Berlin, Germany, 2010.

[31] M. Mambo and E. Okamoto, "Proxy cryptosystems: delegation of the power to decrypt ciphertexts," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences,* vol. 80, no. 1, pp. 54-62, 1997.

[32] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," *in Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT '98),* pp. 127-144, Espoo, Finland, 1998.

[33] Guojun Wang, Qin Liu, Jie Wu and MinyiGuo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers", 2011.

[34] Chunpeng Ge, Zhe Liu, Jinyue Xia, and Liming Fang, "Revocable Identity-Based Broadcast ProxyRe-encryption for Data Sharing in Clouds", *IEEETransactions on Dependable and Secure Computing,* 2018.

[35] SumanaMaiti and SudipMisra, "P2B: Privacy Preserving Identity-Based BroadcastProxy Re-encryption", *IEEETransactions on Vehicular Technology,* 2020.

[36] JieCui, HanZhou, HongZhong, "AKSER: Attribute-based keyword search with efficient revocation in cloud computing", *Information Sciences,* vol. 423, pp. 343-352, 2018.

[37] Jie Cui, Xiaoyu Zhang, Hong Zhong, "Extensible Conditional Privacy Protection Authentication Scheme for Secure Vehicular Networks in a Multi-Cloud Environment", *IEEE Transactions on Information Forensics and*

Security, vol. 15, 2019.

[38] Jin Li, YinghuiZhang, XiaofengChen, "Secure attribute-based data sharing for resource-limited users in cloud computing", *Computers & Security*, vol. 72, pp. 1-12, 2018.

[39] Jing Wang, Libing Wu, Kim-Kwang Raymond Choo, Debiao He, "Blockchain-Based Anonymous Authentication with Key Management for Smart Grid Edge Computing Infrastructure", *IEEE Transactions on Industrial Informatics*, vol. 16, issue 3, 2020.

[40] Wei Li, Li Xuelian, Juntao Gao, Hai Yu Wang, "Design of Secure Authenticated Key Management Protocol for Cloud Computing Environments", *IEEE Transactions on Dependable and Secure Computing*, 2019.

[41] Jie Cui, Han Zhou, Yan Xu, Hong Zhong, "OOABKS: Online/offline attribute-based encryption for keyword search in mobile cloud", *Information Sciences*, vol. 489, pp. 63-77, July 2019.

[42] Maosheng Sun, Chunpeng Ge, "A proxy broadcast re-encryption for cloud data sharing", *Multimedia Tools and Applications*, 2017.

[43] Arij Ben Amor, M. Abid, A. Meddeb, "A Privacy-Preserving Authentication Scheme in an Edge-Fog Environment", *International Conference on Computer Systems and Applications*,2017.

[44] Khalid Mahmood,Arun Kumar Sangaiah, "Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure", *Computer Systems*, 2018.

[45] Hu Xiong,HaoZhang,Jianfei Sun, "Attribute-Based Privacy-Preserving Data Sharing for Dynamic Groups in Cloud Computing", *IEEE Systems Journal*, vol. 13, issue 3, 2019.

[46] R. V. Mante, Nikhil R. Bajad, "A Study of Searchable and Auditable Attribute Based Encryption in Cloud", *International Conference on Communication and Electronics Systems*, 2020.

[47] Van-HoanHoang,ElyesLehtihet, "Forward-Secure Data Outsourcing Based on Revocable Attribute-Based Encryption", *International Wireless Communications & Mobile Computing Conference*, 2019.

[48] Kai Fan, QiangPan,Kuan Zhang, "A Secure and Verifiable Data Sharing Scheme Based on Blockchain in Vehicular Social Networks", *IEEE Transactions on Vehicular Technology*,Vol. 69, Issue 6, June 2020.

[49] Emanuele Bellini, Paolo Ceravolo, Ernesto Damiani, "Blockchain-Based E-Vote-as-a-Service", *IEEE 12th International Conference on Cloud Computing (CLOUD)*, 2019.

[50] Gang Wang, Zhijie Shi, Mark Nixon, Song Han, "ChainSplitter: Towards Blockchain-Based Industrial IoT Architecture for Supporting Hierarchical Storage", *IEEE International Conference on Blockchain (Blockchain)*, 2019.

[51] Yuzhe Tang, QiwuZou, Ju Chen, Kai Li, Charles A. Kamhoua, Kevin Kwiat, Laurent Njilla, "ChainFS: Blockchain-Secured Cloud Storage", *IEEE 11th International Conference on Cloud Computing (CLOUD)*, 2018.

[52] ShorouqAlansari, Federica Paci, Andrea Margheri,VladimiroSassone, "Privacy-

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 180 - 192
Received 16 February 2021; Accepted 08 March 2021.

Preserving Access Control in Cloud Federations", *IEEE 10th International Conference on Cloud Computing (CLOUD),* 2017.

[53] Wenbin Zhang, Yuan Yuan,Yanyan Hu, "A Privacy-Preserving Voting Protocol on Blockchain", *IEEE 11th International Conference on Cloud Computing (CLOUD),* 2018.