Pegem Journal of Education and Instruction, Vol. 13, No. 4 , 2023 (pp. 695-708)

RESEARCH ARTICLE WWW.PEGEGOG.NET

AN EFFICIENT POST-QUANTUM ATTRIBUTE BASED ENCRYPTION SCHEME BASED ON RANK METRIC CODES FOR CLOUD COMPUTING

I.Anusha[1], K Sai Vaishnavi Reddy [2],K.Hema Gayatri [3], Ms. M. Thanmai Reddy[4]

[1] Assistant Professor, Department of Information Technology, Sridevi Women's Engineering College, Hyderabad

igantianusha@gmail.com

[2, 3, 4] Department of Information Technology, Sridevi Women's Engineering College, Hyderabad

ABSTRACT

One useful method for protecting sensitive information in the cloud is attribute-based encryption. The data owner may safely store and exchange data inside the cloud environment using this cryptographic primitive. However, quantum computers have come a long way in the last few years, and this has sparked optimism that we may finally be able to solve some of mathematics's most perplexing issues, such as decimal factoring and calculating discrete logarithms of big numbers. New encryption protocols are very vulnerable to attacks from quantum computers. Verifiability, user privacy, and user revocability are three crucial requirements that have not been concurrently met by existing post-quantum attribute-based encryption techniques. Using rank metric codes, we provide the first post-quantum attribute-based encryption system that is both secure and practical. Because we use low rank parity check codes in our scheme, we get all the benefits listed above. In addition to protecting against selected ciphertext attacks, the suggested system also protects against response attacks, which are a kind of chosen plaintext assaults in the conventional model. Also, on a PC, the execution time is roughly 31.2 ms, and the key size is about 16.5 KB, all at the 256-bit security level. Based on our implementation findings, the suggested method outperforms both conventional and post-quantum techniques that are already in use.

KEYWORDS: Attribute-based encryption, cryptographic primitive, discrete logarithms, post-quantum, ciphertext attacks.

1. INTRODUCTION

When establishing an encrypted connection via a public key network, it is crucial to swap out each user's public key. Consequently, it is crucial that there be an authority in place to either provide or revoke public and private keys for

How to cite this article: I.Anusha1, K Sai Vaishnavi Reddy 2,K.Hema Gayatri 3, Ms. M. Thanmai Reddy4. AN EFFICIENT POSTQUANTUM ATTRIBUTE BASED ENCRYPTION SCHEME BASED ON RANK METRIC CODES FOR CLOUD COMPUTING.Pegem Journal of Education and Instruction, Vol. 13, No. 4, 2023, 695-708

Source of support: Nil **Conflicts of Interest:** None.

DOI: 10.48047/pegegog.13.04.79

Received: 12.10.2023

Accepted: 22.11.2023 **Published:** 24.12.2023

applicants. A framework for maintaining certificates and validating user identities, the public key infrastructure has been built for this

aim to offer a safe environment. Each user's public key may be produced using their identification, eliminating the requirement to generate a certificate for the public key. In 1984, Shamir first suggested what is now known as identity-based encryption (IBE). Users don't need to get the public key from the certificate provided by a trustworthy authority as the private keys are already generated for them based on their ID. Boneh and Franklin presented the first workable plan for IBE in 2001. One major benefit of IBE is that after all users are registered, the trusted authority's private key is deleted. Then there'll be no more need for a major distribution hub. Following the lead of IBE, Sahai and Waters created the first attribute-based encryption (ABE) system. Fuzzy ID-based encryption was the name they gave to their technique. The original Sahai and Waters technique relies on the closeness of two sets of characteristics as its system policy for decryption. This policy may benefit from being more convenient, even if it is straightforward. The policy was created based on further study. Key policy ABE (KP-ABE) and cipher text policy ABE (CP-ABE) are the two main varieties of ABE policies. According to KP ABE, the sender encrypts the message with the specified characteristics, and the receiver's private key is defined according to the desired access structure. Instead of the receiver generating his private key based on his qualities, with CPABE it is the data sender that encrypts the data using the appropriate access structure.More and more people are thinking about moving their data storage and processing to the cloud in order to increase processing speed, decrease hardware maintenance expenses, and increase data storage capacity. Users cannot fully trust the cloud server, thus data is often encrypted before being saved in the cloud. Since this is a serious issue, one of the main challenges is figuring out how to let different users safely exchange data according to a policy. The good news is that ABE has a simple answer to this dilemma. More recent updates to ABE have included capabilities like verifying the outcomes of outsourced computations and the ability to cancel user

access.The efficiency is reduced since these systems rely on elliptic curve pairing. In addition to greatly improving efficiency, this issue has already been resolved in. Recent years have seen quantum computers undergo significant development. Many current cryptographic methods, such RSA and DSA, have their security broken when using Shor's quantum algorithm and supposing to construct powerful enough quantum computers. In response to the potential dangers posed by quantum computers, the NIST initiated a procedure to establish uniform standards for asymmetric encryption, key exchange, and digital signature methods. To improve data security in cloud computing settings, several ABE systems have been suggested, all of which depend on number theoretic issues. The problem is that quantum computers can crack all of them. To protect themselves against quantum computers, ABE systems based on lattices have recently been suggested. But these methods might need some efficiency improvements since their key lengths are so long. We provide a rank metric code based post-quantum ABE method that is both semantically safe and efficient with respect to key length and complexity of encryption/decryption time as a function of the number of attributes. As an improved and more efficient substitute for Hamming metric codes in cryptography applications, rank metric codes have recently attracted a lot of interest. We use rank metric codes for ABE design since they have the right key-length and work well. We base our suggested technique on CP-ABE because in realworld data-sharing applications, the sender should be able to choose the access structure. Bloom filter forms the basis of the proposed scheme's access structure. An element's membership in a set may be checked using a hash-based data structure called a bloom filter. In this paper we introduce a novel type of cryptographic scheme, which enables any pair of users to communicate securely and to verify each other‟s signatures without exchanging private or public keys, without keeping key directories, and without using the services of a third party. The scheme assumes the existence of trusted key generation centers, whose sole purpose is to give each user a personalized smart card when he first joins the network. The information embedded in this card enables the user to sign and encrypt the messages he sends and to decrypt and verify the messages he receives in a totally independent way, regardless of the identity of the other party. Previously issued cards do not have to be updated when new users join the network, and the various centers do not have to coordinate their activities or even to keep a user list. The centers can be closed after all the cards are issued, and the network can continue

to function in a completely decentralized way for an indefinite period.We propose a fully functional identity-based encryption scheme (IBE). The scheme has chosen ciphertext security in the random oracle model assuming a variant of the computational DiffieHellman problem. Our system is based on bilinear maps between groups. The Weil pairing on elliptic curves is an example of such a map. We give precise definitions for secure identity based encryption schemes and give several applications for such systems In 1984 Shamir [41] asked for a public key encryption scheme in which the public key can be an arbitrary string. In such a scheme there are four algorithms: (1) setup generates global system parameters and a master-key, (2) extract uses the master-key to generate the private key corresponding to an arbitrary public key string ID $\in \{0,1\}*$, (3) encrypt encrypts messages using the public key ID, and (4) decrypt decrypts messages using the corresponding private key. Shamir‟s original motivation for identity-based encryption was to simplify certificate management in e-mail systems. When Alice sends mail to Bob at

bob@company.com she simply encrypts her message using the public key string "bob@company.com". There is no need for Alice to obtain Bob"s public key certificate. When Bob receives the encrypted mail he contacts a third party, which we call the Private Key Generator (PKG). Bob authenticates himself to the PKG in the same way he would authenticate himself to a CA and obtains his private key from the PKG. Bob can then read his e-mail. Note that unlike the existing secure e-mail infrastructure, Alice can send encrypted mail to Bob even if Bob has not yet setup his public key certificate. Also note that key escrow is inherent in identity-based e-mail systems: the PKG knows Bob"s private key. We discuss key revocation, as well as several new applications for IBE schemes in the next section. Since the problem was posed in 1984 there have been several proposals for IBE schemes [11, 45, 44, 31, 25] (see also [33, p. 561]). However, none of these are fully satisfactory. Some solutions require that users not collude. Other solutions require the PKG to spend a long time for each private key generation request. Some solutions require tamper resistant hardware. It is fair to say that until the results in [5] constructing a usable IBE system was an open problem. Interestingly, the related notions of identity-based signature and authentication schemes, also introduced by Shamir [41], do have satisfactory solutions [15, 14]. In this paper we propose a fully functional identity-based encryption scheme. The performance of our system is comparable to the performance of ElGamal encryption in F_p^*. The security of our system is based on a natural analogue of the computational Diffie-Hellman assumption. Based on this assumption we show that the new system has chosen ciphertext security in the random oracle model. Using standard techniques from threshold cryptography [20, 22] the PKG in our scheme can be distributed so that the master-key is never available in a single location. Unlike common threshold systems, we show that robustness for our distributed PKG is free. Our IBE system can be built from any bilinear map $e : G1 \times G1 \rightarrow G2$ between two groups G1,G2 as long as a variant of the Computational Diffie-Hellman problem in G1 is hard. We use the Weil pairing on elliptic curves as an example of such a map. Until recently the Weil pairing has mostly been used for attacking elliptic curve systems [32, 17]. Joux [26] recently showed that the Weil pairing can be used for "good" by using it for a protocol for three party one round Diffie-Hellman key exchange. Sakai et al. [40] used the pairing for key exchange and Verheul [46] used it to construct an ElGamal encryption scheme where each public key has two corresponding private keys. In addition to our identity-based encryption scheme, we show how to construct an ElGamal encryption scheme with "built-in" key escrow, i.e., where one global escrow key can

decrypt ciphertexts encrypted under any public key. To argue about the security of our IBE system we define chosen ciphertext security for identitybased encryption. Our model gives the adversary more power than the standard model for chosen ciphertext security [37, 2]. First, we allow the attacker to attack an arbitrary public key ID of her choice. Second, while mounting a chosen ciphertext attack on ID we allow the attacker to obtain from the PKG the private key for any public key of her choice, other than the private key for ID. This models an attacker who obtains a number of private keys corresponding to some identities of her choice and then tries to attack some other public key ID of her choice. Even with the help of such queries the attacker should have negligible advantage in defeating the semantic security of the system.Vehicular ad hoc networks (VANETs) are becoming the most promising research topic in intelligent transportation systems, because they provide information to deliver comfort and safety to both drivers and passengers. However, unique characteristics of VANETs make security, privacy, and trust management challenging issues in VANETs‟ design. This survey article starts with the necessary background of VANETs, followed by a brief treatment of main security services, which have been well studied in other fields. We then focus on an in-depth review of anonymous authentication schemes implemented by five pseudonymity mechanisms. Because of the predictable dynamics of vehicles, anonymity is necessary but not sufficient to thwart tracking an attack that aims at the drivers‟ location profiles. Thus, several location privacy protection mechanisms based on pseudonymity are elaborated to further protect the vehicles‟ privacy and guarantee the quality of location-based services simultaneously. We also give a comprehensive analysis on various trust management models in VANETs. Finally, considering that current and near-future applications in VANETs are evaluated by simulation, we give a much-needed update on the latest mobility and network simulators as well as the integrated simulation platforms. In sum, this paper is carefully positioned to avoid overlap with existing surveys by filling the gaps and reporting the latest advances in VANETs while keeping it self-explained. I N RECENT years, intelligent transportation systems (ITSs) [1] have gained a lot of popularity in both industry and academia. In addition to providing entertainment services on vehicles, the main motivation of ITSs is to improve road safety and driving conditions [2]. In order to share the critical driving information, vehicular ad hoc networks (VANETs) are established with two types of communication, namely vehicle-tovehicle (V2V) and vehicles-to-infrastructure (V2I) communication [3]. As shown in Fig. 1, in V2V communication, vehicles communicate with nearby vehicles to exchange information; and in V2I communication, vehicles communicate directly with roadside units (RSUs) [4].

Dedicated short

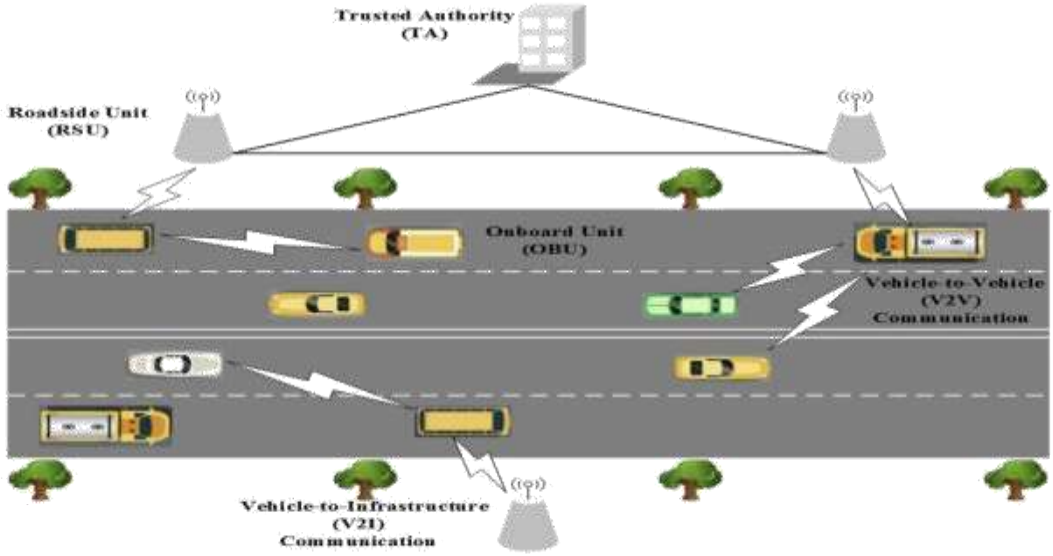


Fig. 1. System model of vehicular ad hoc networks (VANETs).

range communication (DSRC) radio [5] and a couple of IEEE standards can be used for V2V and V2I communications in VANETs. Unique characteristics such as high mobility and volatility of VANETs have made it vulnerable to various kinds of external and internal attacks

[6]. These attacks have caused three main concerns in the design of secure VANETs: security, privacy and trust. Many researchers have proposed various methods to ensure security, preserve privacy and establish trust management for VANETs. Several excellent surveys have been published in recent years, which all cover the background of VANETs such as the requirements, challenges, different types of threats and corresponding solutions. However, each survey has its own emphasis and shortcomings. The 2014 survey by Engoulou et al. [6] summarizes characteristics and challenges of VANETs and proposes solutions to various security issues but with little coverage on privacy-preserving methods. Another 2014 survey by Al-Sultan et al. [7] gives a comprehensive treatment on VANETs that starts from the architecture and concludes with simulation tools, simulate protocols and applications. Many new simulation tools have been developed since then and Section VII in this article can be considered an update. The 2015 review by Qu et al. [8] and the 2016 survey by Azees et al.

[4] focus on the authentication methods with conditional privacy preservation in addition to common security concerns. This survey is complementary to the above work in that we focus on

topics that they did not cover and new results reported in the past several years. Meanwhile, for the convenience of readers of different background, we try to make this survey self-contained by covering the fundamentals of VANETs and all three security related topics. With this goal in mind, after a short review of the system model, communication patterns, and other characteristics of VANETs in Section II, we cover VANETs security, trust,

and privacy as follows: well-studied security topics are covered without detailed elaboration; discussion on privacy features the less-covered anonymous authentication schemes and location privacy protection mechanisms; a systematic and in-depth survey on VANETs trust management; the latest VANETs simulation tools and platforms are reported.

2. MATERIALS AND MODULES

A cryptographic primitive called public key encryption with keyword search (PEKS) enables a cloud server to securely search for users' preferred keywords with the usage of a search token. We provide the first rank metric code based post-quantum PEKS technique that we are aware of that is both feasible and semantically safe. The current technique is protected against key exposure, response attacks, and keyword guessing. It also has convenient features like conjunctive keyword search, verifiability of search results using Bloom filter, and garbled Bloom filter. We put the plan into action on a desktop computer using the C++ programming language. The technique encrypts data, searches for keywords, and verifies search results for a single term in 22.5 milliseconds at a 256-bit security level. This degree of security also requires a public key length of about 5 kilobytes. We demonstrate that the method outperforms the relevant post-quantum ones that are currently available. Owner of Data He enters his credentials (username and password) to access this section. Once logged in, the data owner may proceed to do the following: Manage your files with ease: upload, delete, and view. Data Subject He enters his credentials (username and password) to access this section. Access Control Response for Private Key, Search, View Files, Download File, Req Download and Decrypt Access Control, View Download and Decrypt Access Control Response, and Private Key Access Control are some of the tasks that the user may do after logging in. Respected Expert Here the Trusted Authority may do tasks including seeing transactions, private keys for files, controlling who can access private keys, and requesting

decryption keys. Data Center When used as a server, the cloud can store data and perform other operations like viewing transactions, users, data owners, files, revoked users, download and decrypt access controls, private key access controls, file rank results, time delay results, and throughput results.

3. DISCUSSION

There is currently no system that uses the proposed attribute-based encryption approach based on rank-metric codes. • Semantically secure, or even CPA-secure, schemes do not exist. It proposes a rank metric code-based post-quantum ABE method that is both semantically safe and efficient with respect to key length and complexity of encryption/decryption time as a function of attribute count. For cryptographic purposes, rank metric codes have recently attracted a lot of interest as an improvement over Hamming metric codes [22], [23], [24]. We are motivated to adopt rank metric codes for ABE design due to their correct key-length and high performance. We base our suggested technique on CP-ABE because in real-world data-sharing applications, the sender should be able to choose the access structure. The suggested scheme's access mechanism is built upon the Bloom filter

[25]. An element's membership in a set may be checked using a hash-based data structure called a bloom filter. This system explains the steps to generate a Bloom filter and verify membership. Our method makes use of LRPC codes, which have the benefit of simple memory requirements for storing the parity check matrix and quick decoding algorithms.

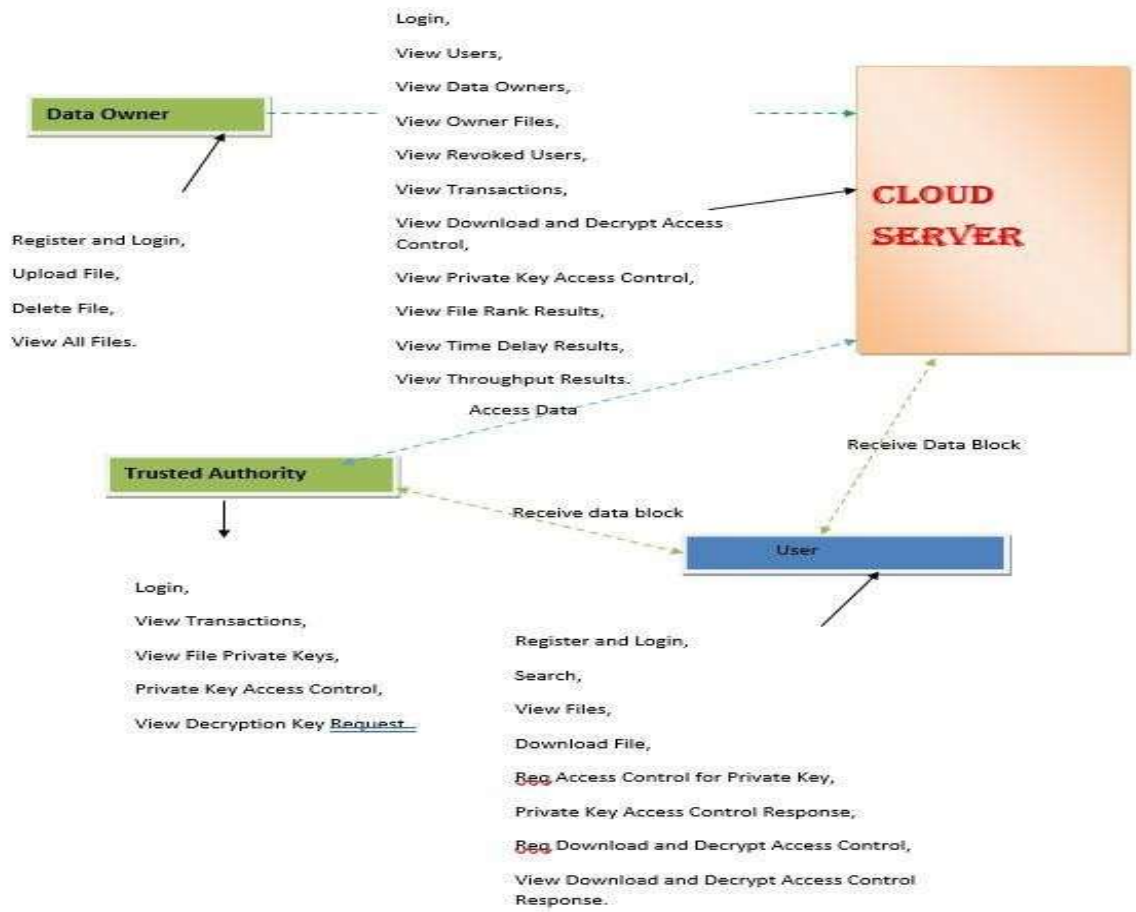
4. RESULT

- Standard model post-quantum security: We have shown our scheme's semantic security by supposing that solving the ideal rank syndrome decoding issue for LRPC codes and LRPC indistinguishability is tough. No algorithm, conventional or quantum, has been suggested as a solution to these issues as of yet.

- Revocation of access by the user: The proposed approach re-encrypts any cloud data that matches the user's characteristics if the user's access is revoked, preventing the revoked user from accessing it.

• Comprehensiveness: The user may easily check whether all of the data stored in the cloud has been searched after obtaining it from the cloud. • User confidentiality: All user-submitted data search requests are encrypted before transmission to the cloud server using the user's key. Consequently, the user's characteristics remain hidden from the cloud server while it searches for the requested data. • Appropriate key length and efficient implementation: The suggested approach relies heavily on linear operations on LRPC codes and hash functions for almost all of its computations. As a result, when contrasted with both classical and post-quantum schemes, the suggested one is more efficient. The suggested scheme's key, for a 256-bit security level, is around 16.5 KB in length, which is commensurate with current technological standards and allows for its use in a variety of contexts.

SYSTEM ARCHITECTURE



RESULTS HOME PAGE

Enter the Required Values in The Field for login purpose

CLOUD LOGIN PAGE

Enter the Required Values in The Field for login purpose

TRUSTED AUTHORITY LOGIN PAGE

Enter the Required Values in The Field for login purpose

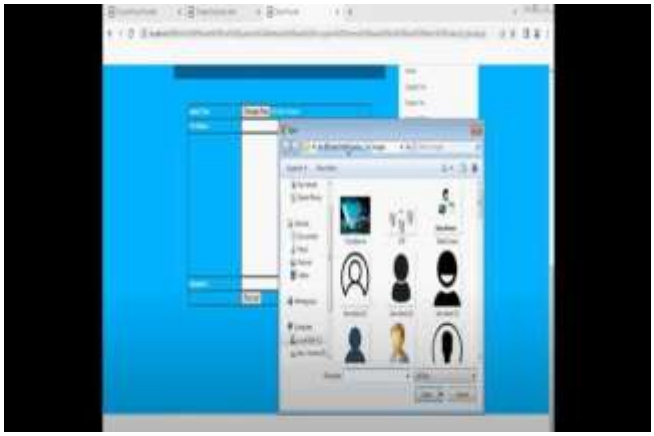
DATA OWNER REGISTRATION PAGE

Enter the Required Values in The Field

DATA OWNER LOGIN PAGE

Enter the Required Values in The Field for login purpose

UPLOAD FILE



UPLOADING DATA

ENCRYPTING DATA

After Encrypting the file owner is going to upload data to cloud

FILE RANKS

5. CONCLUSIONS

We believe our proposal to be the first rank metric code-based attribute-based encryption system. Low rank parity check code is the basis of the suggested technique. Therefore, the suggested technique is efficient, uses a minimal key size, and is provably secure against the specified keyword attack. Its robustness stems from the fact that neither classical or quantum algorithm has been able to handle the challenging LRPC indistinguish ability and ideal rank syndrome decoding issues in polynomial time. Additional security is provided by its resistance to response attacks, a kind of selected cipher text attack. Revocation by the user is ensured by the suggested approach. If a user tries to access a database that is already encrypted, the cloud server will re-encrypt the whole database. Without requiring the user to alter their key, the re-encryption procedure is quick. The user may ensure that the data obtained from the cloud server is accurate and comprehensive by using the Bloom filter in the suggested method. The scheme's desktop execution time is 31.2 ms, and the key size is about

16.5 KB, when using a 256-bit security level. Based on our implementation findings, the suggested method outperforms both conventional and post-quantum schemes in terms of efficiency. Take note that we have tested the suggested scheme's robustness against response attacks, a subset of cipher text assaults. Still, more work has to be done to prove that the proposed system is secure against attacks on selected cipher texts.

6. REFERENCES AND CITATION

[1] S. Choudhury, K. Bhatnagar, and W. Haque, *Public Key Infrastructure Implementation and Design*. Hoboken, NJ, USA: Wiley, 2002.

[2] A. Shamir, „„Identity-based cryptosystems and signature schemes,“‘‘ in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1984, pp. 47–53.

[3] D. Boneh and M. Franklin, „„Identity-based encryption from the Weil pairing,“‘‘ in *Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 2001, pp. 213–229.

[4] Z. Lu, G. Qu, and Z. Liu, „„A survey on recent advances in vehicular network security, trust, and privacy,"" *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2019.

[5] A. Sahai and B.Waters, „„Fuzzy identity-based encryption,"" in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Springer, 2005, pp. 457–473.

[6] J. Li, Y. Zhang, X. Chen, and Y. Xiang, „„Secure attribute-based data sharing for resource-limited users in cloud computing,"" *Comput. Secur.*, vol. 72, pp. 1–12, Jan. 2018.

[7] M. Ali, S. U. Khan, and A. V. Vasilakos, „„Security in cloud computing: Opportunities and challenges,"" *Inf. Sci.*, vol. 305, pp. 357–383, Jun. 2015.

[8] Y. Yu, J. Shi, H. Li, Y. Li, X. Du, and M. Guizani, „„Key-policy attributebased encryption with keyword search in virtualized environments,"" *IEEE J. Sel. Areas Commun.*, vol. 38, no. 6, pp. 1242–1251, Jun. 2020.

[9] T. V. X. Phuong, G. Yang, and W. Susilo, „„Hidden ciphertext policy attribute-based encryption under standard assumptions,"" *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, pp. 35–45, Jan. 2016.

[10] V. Yousefipoor, M. H. Ameri, J. Mohajeri, and T. Eghlidos, „„A secure attribute-based keyword search scheme against keyword guessing and chosen keyword attacks,"" *Int. J. Inf. Commun. Technol. Res.*, vol. 10, no. 1, pp. 48–55, 2018.

[11] T. Alam, "Cloud computing and its role in the information technology", *IAIC Trans. Sustain. Digit. Innov.*, vol. 1, no. 2, pp. 108-115, 2020.

[12]. K. Fan, T. Liu, K. Zhang, H. Li and Y. Yang, "A secure and efficient outsourced computation on data sharing scheme for privacy computing", *J. Parallel Distrib. Comput.*, vol. 135, pp. 169-176, Jan. 2020.