Indonesian Journal of Electrical Engineering and Computer Science
Vol. 30, No. 1, April 2023, pp. 129~136
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v30.i1.pp129-136

Cost-effective anonymous data sharing with forward security using improved authentication

Shubhangi Handore[1], Pallavi Kolapkar[1], Pratibha Chavan[1], Pramod Chavan[2]
[1]Department of Electronics, Trinity College of Engineering and Research, Pune, India
[2]Department of Electronics and Telecommunication, KJ College of Engineering and Management Research, Pune, India

Article Info

Article history:

Received Jul 12, 2022
Revised Oct 11, 2022
Accepted Nov 18, 2022

Keywords:

Cloud computing
Data sharing
Encryption
Forward security
ID-based ring signature

ABSTRACT

Cloud computing gives customers instant access to a network of remote servers, networks, and data centres. Cloud computing makes data analysis helpful to society and individuals. Sharing data with many people causes efficiency, integrity, and privacy issues. Ring signatures may enable secure and anonymous data transfer. It anonymizes data verification for cloud-based analytics. Identity-based (ID) ring signatures are becoming popular alternatives to public key infrastructure (PKI)-based public-key encryption. PKI bottlenecks are certificate verification time and cost. ID-based ring signatures speed up certificate verification. We observed that encrypting ID-based ring signatures with a variation of SHA-384 and adding forward security considerably improves their security. Padding divides the input text into 512-byte blocks and adds the length as a 48-bit value to the hash in newer SHA versions. Signatures made before a user's secret key was compromised are legitimate. If a user's secret key is compromised, it's impossible to compel all data owners to re-verify their data, hence a large-scale data sharing system must contain this feature. We implement, secure, and prove our method's use. SHA-384 is safer for cloud-based anonymous data sharing.

Corresponding Author:

Pratibha Chavan
Department of Electronics, Trinity College of Engineering and Research
Pune, India
Email: pratibhachavan.tcoer@kjei.edu.in

1. INTRODUCTION

The popularity and broad usage of "CLOUD" have facilitated the sharing and collecting of data in several ways [1]-[3]. Not only may people access relevant data more quickly, but sharing data with others has several advantages for our society [4]-[6]. As an illustration, users in smart grid [7] may receive their energy usage data in granular detail and are encouraged to share it sharing it with others, for instance by posting it on a third-party site like Microsoft Hohm [8]. In Figure 1. A statistical report is generated from the collected data, allowing for the comparison of energy use to that of similar establishments (e.g., from the same block). Improved energy efficiency is possible when data from all parts of the electric grid can be accessed, analyzed, and acted upon.

Because of its open nature, data sharing is typically carried out in a dangerous setting and is prone to several security threats. Several security goals, using smart grid data exchange as an example, must be met by a practical system: i) data authenticity: opponents' fabricated energy use data in the context of a smart grid would be misleading. Existing cryptographic methods (such message authentication codes or digital signatures) can be used to solve this issue, but there may be additional complexities when other factors, like anonymity and efficiency, are taken into account; ii) anonymity: energy consumption records contain a wealth of information about customers, including, for example, the number of occupants in a home, and the kinds of electric appliances used at a given time. Customers' anonymity in these applications must be protected at all costs to prevent them from being dissuaded from using them; iii) efficiency: consider a smart grid that spans an entire country; with so many users, the system's computation and communication costs would need to be as low as possible for it to be economically viable. The smart grid will be useless if energy is wasted.

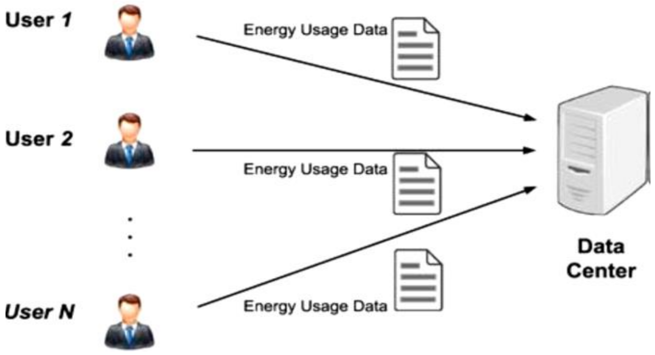


Figure 1. Energy used data sharing in smart grid

This study investigates fundamental security mechanisms for achieving the three mentioned criteria. We used a modified SHA-384 algorithm to the current identity-based (ID) ring signature, which proved to be more secure when evaluated under real-time conditions, to enhance the security work. The following is a summary of the key contribution of this study.

- We present a new concept referred to as forward secure ID-based ring signature, which is a crucial component for constructing cost-effective genuine and anonymous data exchange systems.
- First formal definitions of conveying safe ID-based ring signatures with enhanced, modified SHA384 encryption technique are presented.
- We demonstrate the security of the proposed method in the random oracle model under the conventional RSA assumption with a modified new encryption algorithm using a modified novel encryption algorithm.

2. METHOD

The aforementioned three problems bring to mind the cryptographic primitive "identity-based ring signature," a practical approach to protecting the privacy and integrity of data in contexts where such protections are essential. In this section, we are describring the methodologies and the algorithms we had used to build our system. The main part is encryption system which is mentioned in section 2.1 followed by the mathematical equations in further section.

2.1. ID-based cryptosystem

Shamir [9] public-key certificate authentication is a time-consuming and resource-intensive process that can be avoided with the adoption of an ID-based cryptosystem. Each user's public key in an ID-based cryptosystem can be easily calculated from a string that corresponds to their known identity (e.g., a residential address, and an email address). A private key generator (PKG) uses the master secret as input to produce unique private keys for each user. Every user in the system effectively has a public key thanks to this feature, which means certificates aren't required (unlike in conventional PKI) (user identity). However, unlike the more popular public key-based signature, an ID-based signature can be verified without first verifying the signer's certificate.

By doing away with the need to validate certificates, the verification process can proceed more quickly and efficiently, which is especially helpful when dealing with a large number of users (example: exchanging information about energy consumption in a smart grid). Protecting the anonymity of the person who created the signature is a primary feature of the ring signature, which is a group-oriented signature. Someone can sign on behalf of a group without the other members of that group knowing they are being enlisted. A message signed by a member of this group (also known as the Rings) can fool any verifier into thinking it was signed by one of their number, in which the true author's name is concealed.

Whistleblowing is one potential application of ring signatures [10], authentication of ad hoc group members' anonymity [11], [12], and a number of other uses that necessitate signer anonymity but don't call for a time-consuming group setup process. Considering the fact that ring signature first showed up in 1994 [13] and its official debut in 2001 [10], several other schemes have been presented [14]-[17]. Big data has a huge advantage particularly in the context of huge data analytics, the ID-based implementation of ring signature has a number of advantages over the traditional public key implementation. Assuming 10,000 users are part of the ring, a standard public key-based ring signature would need the verifier to first authenticate 10,000 certificates of linked users before verifying the message and signature.

In contrast, when verifying a ring signature based on user IDs, only the ring user IDs, the message, and the signature pair are required. Certificate validation is a time-consuming and labor-intensive process that can be avoided. These cost reductions become even more important if a greater degree of anonymity is desired simply adding more people to the circle. Figure 2 illustrates this point by showing how ID-based ring signatures are favored in high-traffic settings such as smart grid energy data transmission. To begin, the owner of the energy data (we'll call him Bob) chooses a group of users to form a ring.

Step 1: Bob needs only the members' public identifying information, includes their residential addresses, without the help (or consent) of any members of the ring.

Step 2: Bob uploads his electronic usage-related personal information, as well as a ring signature and individual member details.

Step 3: By validating the ring signature, one may be certain that the data was handed out by a legitimate resident (among the ring members) without being able to identify the resident. Consequently, both the anonymity of the data source and the veracity of the data is assured. In the meantime, the verification is efficient and requires no certificate verification. The first ID-based ring signature technique that can be proven safe in the random oracle model was developed in 2002 [18].

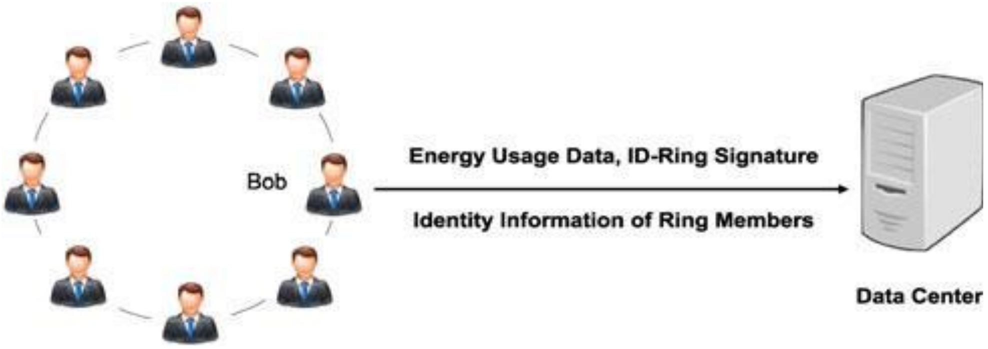

Bob
Energy Usage Data, ID-Ring Signature
Identity Information of Ring Members
Data Center

Figure 2. A method utilising a unique identifier ring signature

Two typical model structures were presented in [19]. However, their initial construction was found to be incorrect [20], [21], and their second design is only proven secure in a lesser model, the selective-ID model. Han *et al.* [22] are responsible for the first ID-based ring signature system stated to be safe in the standard model under the trusted setup assumption.

2.2. Key exposure

Ordinary digital signatures have a basic limitation: once a signer's secret key is compromised, all of that signer's signatures become invalid. Considering that any communication may be forged if the secret key is exposed, this threat may become fairly plausible. This breach invalidates all future signatures, and more critically, none of the previously issued signatures may be trusted. Once a leak has been found, a key revocation mechanism may be implemented immediately to prohibit the creation of signatures using the leaked secret key. However, this does not eliminate the problem of prior signature forgery. Due to several physical and practical restrictions, it is impossible to require the signer to reissue all past signatures.

With a ring signature approach, key disclosure is a particularly serious issue. If an attacker has access to a user's secret key when using an in-ring, signing mechanism, he can not only create a standard digital signature for any document and also sign any document on the group's behalf. Due to the spontaneity of ring signature methods, the adversary can also define the group. The disclosure about one user's secret key not only necessitates changing the public public keys for the entire group, but also invalidates all previously obtained ring signatures because it is impossible to distinguish between such a signature generated by an adversary after gaining one of the secret keys as well as a signature generated by a legitimate user even before adversary obtained one of the secret keys.

The fundamental exposure restriction of digital signatures is supposed to be addressed by forward-secure signature systems. In the event that the current secret key is compromised, a forward-secure signature system seeks to keep the validity of earlier signatures intact. An attacker cannot create signatures for earlier periods, even if the secret key for the current period is revealed. In other terms, the forger is unable to create fake signatures on documents referencing earlier times than the exposure. Documents that were signed prior to the disclosure still maintain their integrity. To lessen the harm brought on by the disclosure of any user's secret key in the ring signature, forwarding security is utilised. Therefore, previously formed ring signatures are also still valid and do not need to be regenerated when a secret key is compromised.

3. THEORIES AND APPROACHES

3.1. Mathematical assumption

Definition 1 (RSA Problem): Let $N = pq$, where p and q are two k-bit prime numbers such that $p = 2p' + 1$ and $q = 2q' + 1$ for some primes p', q'. Let e be a prime greater than 2l for some fixed parameter l, such that $gcd(e, (N)) = 1$. Let y be a random element in $Z * N$. We say that an algorithm S solves the RSA problem if it receives an input the tuple (N, e, y) and outputs an element z such that $ze = ymodN$.

3.2. Security model

An ID-based forward secure ring signature (IDFSRS) system uses two probabilistic polynomial-time (PPT) algorithms:

a) Setup: in response to the input of a unary string 1 containing a security parameter, a set of system parameters param, and descriptions of a user secret key space D, a signature space, and a message space M, the method generates a master secret key msk for the third-party PKG.

b) Extract: users can produce a secret key ski,0, D that is good till time t=0 by providing the master secret key msk, a list param of system parameters, and the user's identification IDi0,1*. Time is portrayed by a series of positive numbers. It is implied that the pair (IDi, ski,0) is an input-output pair of extract for the parameters param and msk when we declare that IDi corresponds to ski,0 or ski,0 corresponds to IDi.

c) Update: the method accepts a user secret key for time t as input and outputs a new account secret key for time t+1.

d) Sign: the method creates a signature using a set of system parameters (param), a group size (n) of length polynomial in, a time (t),a set of n user IDs (L = IDi0,1i [1,n]), a message (m), and a secret key (skIIt 2 D II [1, n]).

e) Verify: the function takes a list of system parameters (param), a time (t), a polynomial-length group size (n), a set of n user IDs (L = IDi0,1i [1,n]), and a signature (S), a message (m 2 M), and returns true or false.

f) Correctness: the verification correctness requirement, which states that signatures produced by a reliable signer are confirmed to be invalid with a possibility of zero, should be satisfied by a (1, n) IDFSRS scheme.

3.3. Modified SHA384 algorithm

Similar performance to SHA-256 can be expected from the proposed SHA-384 algorithm. The 384-bit message digest is generated. The new SHA-384 algorithm is based on the same building blocks as the old one, with the addition of a single new 48-bit word, let's call it F. It's a message digest function that's similar to SHA-384, but it's said to be more secure and runs a little slower. In comparison to SHA-384, it generates a message digest that is 42 bits longer, at 432 bits [23].

The proposed SHA-384 algorithm consists of three distinct phases: preprocessing, iterative processing, and output modification. The preprocessing phase includes padding, turning the padded message into such an m-bit block, and deciding where to begin following iterations. A message digest is computed and sent on to the next stage in the iterative process using a simple function in each of the 80 stages.

We describe a new hash algorithm that considerably alters the secure hash algorithm's core function and provides a 432 bit message digest, filling a gap in the market left by the lack of a suitable alternative [24]. A larger message digest is needed to improve the algorithm's security. In the first stage, this is achieved by increasing the number of chaining variables by 64 bits. The size of the message digest grows dramatically in relation to the input value [25].

The round function has also been improved upon. An increased number of XOR operations is used to raise the algorithm's difficulty and, in turn, its security. The rounding function is invoked more frequently. Plus, on each iteration, various variables in the chain are shifted by 15 bits and 30 bits. The randomness of bit changes in succeeding procedures can be enhanced by moving the bits from the end block to the front, following by additional consecutive bits. Using a preprocessing phase and the exor technique, which makes use of well-known functions and constants, SHA-384 calculates a hash.

4. MODULES IMPLEMENTATION

4.1. Cloud service provider

Module one involves developing a user-centric cloud system concept. The cloud service provider component is built throughout this lesson. A public cloud storage service is offered by this company. The stacked-chip scale packages (S-CSP) provides users with a data outsourcing services and stores their data on their behalf. For the purposes of this study, we will assume that S-CSP is available at all times and is equipped with plenty of memory and processing power. Also, it's a vote of confidence in the group.

4.2. Data owners module

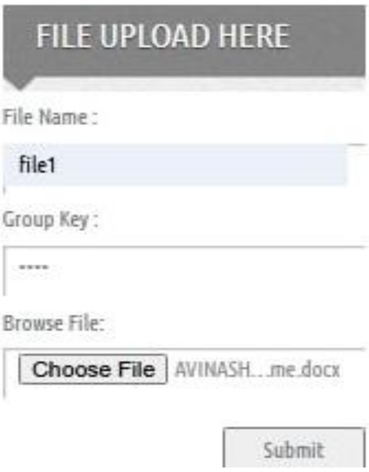
A data owner is a company or organization that wants to store and subsequently retrieve data from the S-CSP. The data's owner places the file in cloud storage. The data owner module is the main integral part of the system. The data owner puts all the files on the cloud storage with all details of patients along with the report of the patients by uploading it in encrypted format on cloud. The other entities of this system will then able to access this information by using authentication scheme developed by us which is controlled by the administrator of the system.

4.3. ID-based ring signature with modified SHA-384

In the beginning, the energy data owner (say, Bob) chooses a group of users to form a ring, and then they begin sharing their data. Bob doesn't need any ring members' cooperation or approval of this step, using just openly available information like home addresses to identify members of the ring. This includes all of Bob's electronic usage statistics, including his modified SHA 384 ring signature. It is possible to validate a resident's identity by confirming the ring signature, but it is impossible to determine who that resident is. Thus, the data provider's anonymity is protected as well as the data's veracity. There is no need for certificate verification for efficient verification.

5. RESULTS AND DISCUSSION

System design provides guidance throughout the early stages of development, when the system is built in modular pieces known as units. Unit testing is the process of creating and verifying the functionality of individual units. The Figure 3 shows the process of uploading the patient's data and access permission given by the administrator respective patient data. Figure 3(a) explains the file upload part where as Figure 3(b) shows the access permission part of shared files.

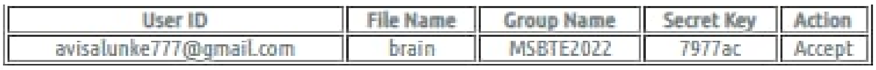

FILE UPLOAD HERE

File Name : file1

Group Key : ****

Browse File: AVINASH....me.docx

(a)

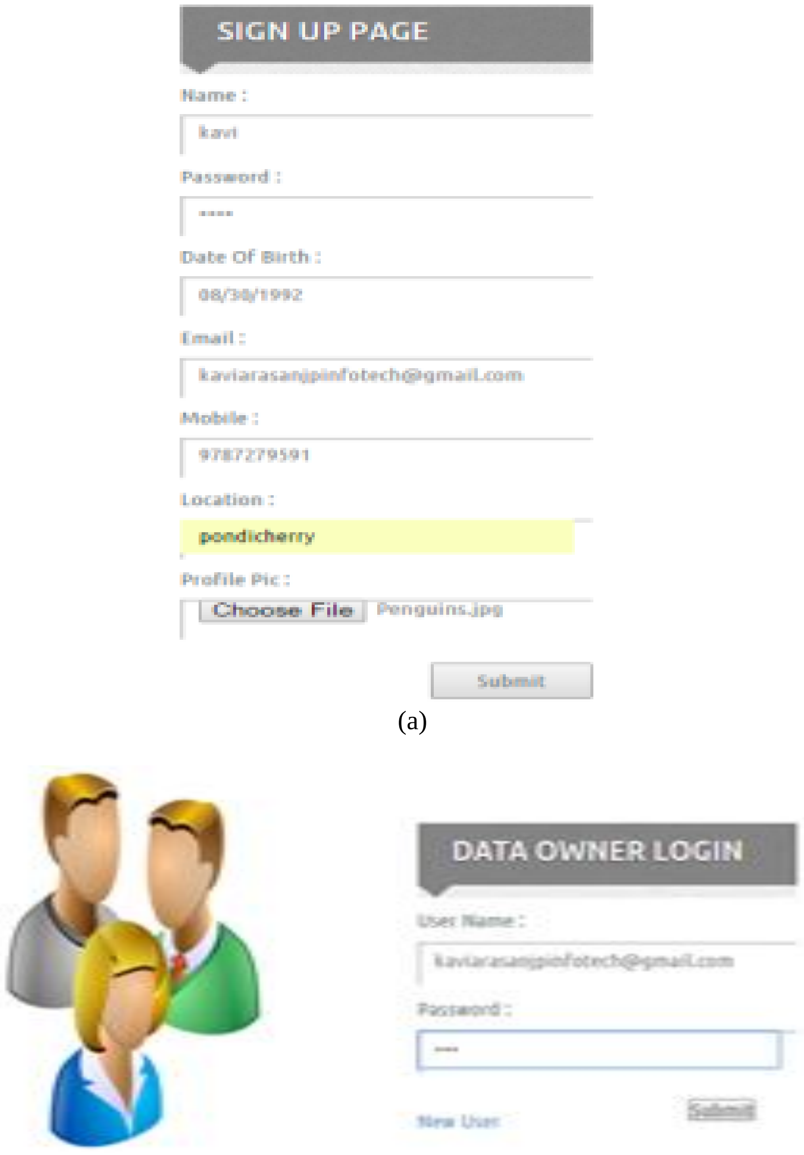


User ID	File Name	Group Name	Secret Key	Action
avisalunke777@gmail.com	brain	MSBTE2022	7977ac	Accept

(b)

Figure 3. Uploading the patient's data (a) file upload and (b) access permission for shared files

Figure 4 gives an overview of user registration and data owner login to access the cloud based system developed under this research. Figure 4(a) represents the file upload page and Figure 4(b) shows the access permission for shared files given by the data owner. Here the modified SHA-384 ID-based ring signature key had been produced as the secret key which is only known and available to the data owner.



SIGN UP PAGE

Name : kavi

Password : ****

Date Of Birth : 08/30/1992

Email : kaviarasanjpinfotech@gmail.com

Mobile : 9787279591

Location : pondicherry

Profile Pic : Choose File Penguins.jpg

Submit

(a)

DATA OWNER LOGIN

User Name : kaviarasanjpinfotech@gmail.com

Password : ****

New User

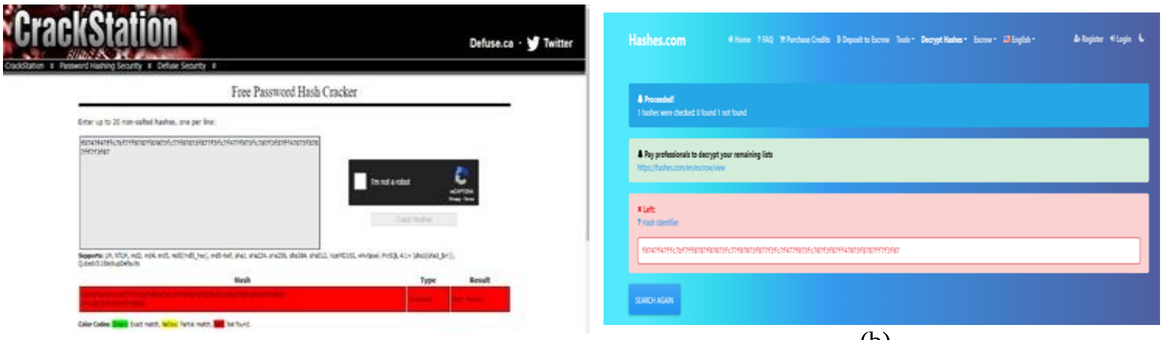
Submit

(b)

Figure 4. Overview to access the cloud based system (a) user registration and (b) data owner login

5.1. Performance analysis of modified SHA-384 algorithm

When we performed the various attacks on the modified SHA-384 algorithm on the generated key and tested through various online simulation software then we found that the secret key generated with the modified SHA-384 ID-based ring signature had not been decrypted. Some results screenshots are shown in the following Figures 5. Figure 5(a) describes the results of our enhanced key encryption mechanism when we tested it on Crackstation. Figure 5(b) describes online simulation results of our proposed encryption algorithm of HashCrack website, then we found that the key generated was not able to crack and hence it proves the security and privacy with an advanced level.


CrackStation
Defuse.ca · Twitter
CrackStation ⇕ Password Hashing Security ⇕ Defuse Security ⇕
I'm not a robot
reCAPTCHA
Crack Hashes
Hashes.com
Home ? FAQ Purchase Credits Deposit to Escrow Tools Decrypt Hashes Escrow English
Register Login
SEARCH AGAIN

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

Hash	Type	Result
[illegible]	[illegible]	[illegible]

Color Codes: Green Exact match, Yellow Partial match, 🟥 Not found.

Proceeded!
1 hashes were checked: 0 found 1 not found

Pay professionals to decrypt your remaining lists
https://hashes.com/en/escrow/view

✖ Left:
? Hash Identifier

(a) (b)

Figure 5. Results of enhanced key encryption mechanism and online simulation results (a) crack station and (b) HashCrack simulation results

6. CONCLUSION

We developed a novel idea termed forward secure ID-based ring signature based on a modified SHA-384 algorithm to meet the actual demands of data sharing. An ID ring signature method can now benefit from forward security. There are no pairing procedures required in our method of computation. When a user's secret key is merely one integer, exponentiation is all that is required to update the key. Much more practical applications, such as ad-hoc networks, e-commerce, and smart grids, will benefit greatly from our system, including those that need user privacy and authentication. The random oracle assumption serves as the foundation for our present scheme's security proof. Proving the security of a system with the same characteristics as the conventional model is still an open question for us and our future research.

REFERENCES

[1] R. Loh and V. L. L. Thing, “Data privacy in multi-cloud: an enhanced data fragmentation framework,” *2021 18th International Conference on Privacy, Security and Trust (PST)*, 2021, doi: 10.1109/PST52912.2021.9647746.

[2] H. Yan and W. Gui, “Efficient identity-based public integrity auditing of shared data in cloud storage with user privacy preserving,” *IEEE Access*, vol. 9, pp. 45822–45831, 2021, doi: 10.1109/ACCESS.2021.3066497.

[3] I. E. Ghoubach, R. B. Abbou, and F. Mrabti, “A secure and efficient remote data auditing scheme for cloud storage,” *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 5, pp. 593–599, Jun. 2021, doi: 10.1016/J.JKSUCI.2019.02.011.

[4] S. Uthayashangar, P. Dhamini, M. Mahalakshmi, and V. Mangayarkarasi, “Efficient group data sharing in cloud environment using honey encryption,” *2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN)*, Mar. 2019, doi: 10.1109/ICSCAN.2019.8878759.

[5] S. Li, J. Liu, G. Yang, and J. Han, “A blockchain-based public auditing scheme for cloud storage environment without trusted auditors,” *Wireless Communications and Mobile Computing*, vol. 2020, 2020, doi: 10.1155/2020/8841711.

[6] M. S. Salek *et al.*, “A review on cybersecurity of cloud computing for supporting connected vehicle applications,” *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8250–8268, Jun. 2022, doi: 10.1109/JIOT.2022.3152477.

[7] R. Leszczyna, “Standards on cyber security assessment of smart grid,” *International Journal of Critical Infrastructure Protection*, vol. 22, pp. 70–89, Sep. 2018, doi: 10.1016/J.IJCIP.2018.05.006.

[8] “Microsoft hohm helps consumers save money and energy - Landis+Gyr.” https://www.landisgyr.eu/news/microsoft-hohm-helps-consumers-save-money-and-energy/ (accessed Jul. 10, 2022).

[9] A. Shamir, “Identity-based cryptosystems and signature schemes,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 196 LNCS, pp. 47–53, 1985, doi: 10.1007/3-540-39568-7_5/COVER/.

[10] R. L. Rivest, A. Shamir, and Y. Tauman, “How to leak a secret,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 2248, pp. 552–565, 2001, doi: 10.1007/3-540-45682-1_32/COVER/.

[11] E. Bresson, J. Stern, and M. Szydlo, “Threshold ring signatures and applications to ad-hoc groups,” *CRYPTO 2002: Advances in Cryptology — CRYPTO 2002*, vol. 2442, pp. 465–480, 2002, doi: 10.1007/3-540-45708-9_30.

[12] X. Wu, H. Ling, H. Liu, and F. Yu, “A privacy-preserving and efficient byzantine consensus through multi-signature with ring,” *Peer-to-Peer Netw. Appl. 2022 153*, vol. 15, no. 3, pp. 1669–1684, Mar. 2022, doi: 10.1007/S12083-022-01317-4.

[13] S. S. M. Chow, S.-M. Yiu, and L. C. K. Hui, "Efficient identity based ring signature," *In International conference on applied cryptography and network security*, pp. 499-512. Springer, Berlin, Heidelberg, 2005.

[14] X. Huang *et al.*, “Cost-effective authentic and anonymous data sharing with forward security,” *IEEE Trans. Comput.*, vol. 64, no. 4, pp. 971–983, 2015, doi: 10.1109/TC.2014.2315619.

[15] X. Peng, K. Gu, Z. Liu, and W. Zhang, “Traceable identity-based ring signature for protecting mobile IoT devices,” In *International Conference on Data Mining and Big Data*, 2021, pp. 158–166.

[16] S. Badrinarayanan, D. Masny, and P. Mukherjee, “Efficient and tight oblivious transfer from PKE with tight multi-user security,” *Cryptology ePrint Archive*, pp. 626–642, 2022.

[17] N. Perera, T. Nakamura, M. Hashimoto, H. Yokoyama, C.-M. Cheng, and K. Sakurai, “A survey on group signatures and ring signatures: Traceability vs. Anonymity,” *Cryptography*, vol. 6, p. 3, Jan. 2022, doi: 10.3390/cryptography6010003.

[18] F. Zhang and K. Kim, “Id-based blind signature and ring signature from pairings,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 2501, pp. 533–547, 2002, doi: 10.1007/3-540-36178-2_33/COVER.

[19] M. H. Au, J. K. Liu, T. H. Yuen, and D. S. Wong, “ID-based ring signature scheme secure in the standard model,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 4266 LNCS, pp. 1–16, 2006, doi: 10.1007/11908739_1/COVER/.

[20] A. Ferrara, M. Green, S. Hohenberger, and M. Pedersen, *Practical Short Signature Batch Verification,* In Cryptographers’ Track at the RSA Conference, pp. 309-324. Springer, Berlin, Heidelberg, 2009.

[21] O. Blazy, L. Brouilhet, E. Conchon, and M. Klingler, “Anonymous attribute-based designated verifier signature,” *Journal of Ambient Intelligence and Humanized Computing*, Mar. 2022, doi: 10.1007/s12652-022-03827-8.

[22] J. Han, X. QiuLiang, and C. Guohua, “Efficient ID-based threshold ring signature scheme,” *2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, vol. 2, pp. 437–442, 2008, doi: 10.1109/EUC.2008.65.

[23] V. Thambusamy and S. Karthiga “Security based approach of SHA 384 and SHA 512 algorithms in cloud environment,” *Journal of Computer Science*, vol. 16, pp. 1439–1450, Oct. 2020, doi: 10.3844/jcssp.2020.1439.1450.

[24] U. Tariq, “Rampant smoothing (RTS) algorithm: An optimized consensus mechanism for private blockchain enabled technologies,” *EURASIP Journal on Wireless Communications and Networking.*, vol. 2022, May 2022, doi: 10.1186/s13638-022-02123-5.

[25] G. Yan, D. Wen, S. Olariu, and M. Weigle, “Security challenges in vehicular cloud computing,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, no. 1, pp. 284–294, Mar. 2013, doi: 10.1109/TITS.2012.2211870.

BIOGRAPHIES OF AUTHORS:

Dr. Shubhangi Handore she is working as Professor and HOD in E&TC department, Trinity College of Engineering and Research, Pune. She completed Ph.D from JJTU, Rajasthan, India and Post Graduate from Pune University. She is having 23 years of experience in the field of teaching and her interest lies in technologies like Image Processing, Signal Processing. In addition, she has published more than 12 papers in the refereed research journals. She can be contacted at email: shubhangihandore.tcoer@kjei.edu.in.

Miss. Pallavi Kolapkar she is studying in E&TC department, Trinity College of Engineering and Research, Pune. She is pursuing ME in Electronics Engineering Department at Trinity College of Engineering and Research, Pune. She completed her Bachelors in E&TC from Pune university. She is having 6 years of teaching experience at Ashok Institute of Engineering Technology, Polytechnic, Shrirampur and her fields of interest are analog and digital communication. She is a member of Professional bodies like IETE. She can be contacted at email: kolapkarpallavi306@gmail.com.

Prof. Pratibha Chavan she is working as Associate Dean (Industry Relations) and PG Coordinator in E&TC department at Trinity College of Engineering and Research, Pune. She is pursuing PhD in Electronics Engineering Department at Sathyabama Institute of Science and Technology, Chennai. She completed her PG in Electronics and Bachelors in E&TC from Pune university. She is having 19 years of teaching and industrial experience and her fields of interest are Image Processing, analog and digital communication. In addition, she has published more than 35 papers in the research journals. She has received a good teacher award “Trinity Ratna Teacher” in January 2019 and 2021. She is a reviewer of Elsevier. She is a member of Professional bodies like IETE, ISTE. She can be contacted at email: pratibhachavan.tcoer@kjei.edu.in.

Dr. Pramod Chavan he is working as Associate Prof and Head of Department E&TC department at KJ College of Engineering and Management Research, Pune. He awarded PhD in Electronics Engineering Department from Sathyabama Institute of Science and Technology, Chennai. He completed his PG and BE E&TC from Pune university. He is having 20 years of experience and his fields of interest are robotics, image processing. In addition, he has published more than 25 papers in the refereed research journals. He is a member of Professional bodies like IETE, ISTE. He can be contacted at email: dr.pu.chavan@gmail.com.