Authentication upon that Blockchain that Is Completely Anonymous Together with Addition To improvements with Distributed Generation Computation Offloading Network

Dr. A. Avani

Assistant Professor, Department of CSE, Anu Bose Institute of Technology, Paloncha, India

avanialla@gmail.com

ABSTRACT

Conventional virtualized smart grid systems have a number of significant obstacles, two of the most significant of which are obtaining low-latency and offering real-time services. As a result, there has been a growing tendency toward shifting toward edge computing. Existing cryptographic methods often do not enable conditional anonymous or flexible identity management, despite the fact that there have been a number of cryptographic protocols developed specifically to make it easier to maintain encrypted systems in smart grid networks.

In light of this, the purpose of this article is to provide a mutual authentication and key negotiation methodology for edge computing-based smart grid systems that is based on blockchain technology. Specifically, by using blockchain technology, the protocol is able to offer efficient conditional anonymity as well as access control. This is accomplished without the use of any extra complicated encryption algorithms. The security analysis demonstrates that the protocol delivers a fair degree of safety assurance. Furthermore, the comparison summary for both safety and efficacy hints that the suggested technique may have use in the context of a power system implementation.

I. INTRODUCTION

One of the many categories of the Industrial Internet of Things (IIoT), smart grid systems are among those that have the potential to increase the dependability, flexibility, and quality of energy distribution [1]. However, when the system grows in size (for example, as the number of customers grows), it may become more difficult to achieve certain goals, such as reducing latency and enhancing quality of service (QoS) [2]. As a result, there have been attempts made to use edge computing to mitigate these challenges, such as utilising electric vehicle charging stations to act as edge computing devices and facilitate real-time decision making, and as a result, improving provisioned quality of service and eco-friendliness in latency-sensitive applications [3, 4]. In addition, there have been attempts made to use edge computing to improve provisioned QoS and eco-friendliness in latency-sensitive applications [5, 6].

It is a well-known cliché that there is no such thing as a completely safe system, and this adage holds true for smart grid security as well.

For instance, the characteristics that are inherent to the architecture of edge computing, such as heterogeneity, mobility, geo-distribution, and location-awareness, can be exploited by attackers to carry out their malicious activities. These characteristics include heterogeneity, mobility, geo-distribution, and location-awareness. In light of this, the

development of workable security solutions for smart grid systems based on edge computing is of the utmost importance, especially in light of the fact that smart grids are becoming more prevalent in technologically sophisticated nations such as the United States.

Verifying the identities of Internet-connected communicators in advance of further interactions allows mutual authentication to be an efficient method for ensuring trust identity and secure communications [5]. This is accomplished without the transmission of sensitive information over an open channel.

The resource limitations of smart metres and other Internet of Things (IoT) devices in the grid make it abundantly evident that traditional public-key infrastructures based protocols are not an appropriate choice for smart grid systems. A large communication overhead and an asynchronous problem are incurred as a result of the dependence on a certificate authority (CA) to issue certificates on a periodic basis and for new devices. Existing identity-based protocols have the ability to eliminate the issue of certificate maintenance; nevertheless, in order to be verified, they need the divulgence of a user's true identity to the other communicator. It is not reasonable to transfer a user's true identity to an edge server since, in general, an edge server has a lower level of security than a centralised cloud and is more vulnerable to assaults. For instance, the possible dangers of identities being compromised in smart grids have been the subject of research in [6].

We may employ ring signature techniques, which are explored in the current body of research [7, 8], to stop the identity from being revealed to the person who is verifying the signature. However, using ring signature techniques in smart grid systems comes with a few significant drawbacks that should be considered.

To begin, it is quite difficult to track down the fraudulent user (for example, in the event that falsified communications are discovered). Second, the high expenses of computing and transmission render it impracticable for devices that are limited in their resource availability. Third, since a ring is always pre-set, it does not permit flexible involvement and so cannot. Blind signature systems are plagued by the identical problems [6]. Even though group signature methods have the potential to enable traceability as well as dynamic involvement, the costs of computation and communication for smart metres are still quite expensive. A mutual authentication protocol will have to provide demonstrable key upgrade and abrogation, particularly in the context of such an edge cloud computing consisting of resource-constrained IoT devices, in order to achieve provisional privacy and confidentiality and facilitate dynamic participation. This is particularly important in the context of an edge computing architecture. Because of this, it is possible to update and revoke private keys before their expiration date in order to safeguard the network. For instance, this may be necessary in the event that events involving private key breach are discovered and the desire to prohibit malevolent metres is imposed. Two common types of revocation tools are the Certificate Revocation List (CRL) and the Online Certificate Status Protocol (OCSP) [9]. The former, on the other hand, has major communication costs and an issue with asynchrony, whereas the second has to be online at all times in order to validate the certificates. In plenty of other words, "how can we accomplish qualities such as conditional anonymity, permitting

dynamic participation, key update and revoke through authentication and authorization in an effective and efficient manner?"

In this work, in an effort to provide a solution to the issue that was just posed, we build a blockchain-based anonymous authentication and key agreement protocol for a smart grid system that is based on edge computing. To be more specific, only edge servers would be required to join the blockchain system in such a system, although end users (such smart metres) would not be required to do so. This prohibits information about a user's identity from being sent to the edge server. A further benefit of the identity-based registration is that the addition of new end users or their departure will not have any impact on the current end users. The new conditional traceability and revocability are provided by the protocol that has been presented. To be more specific, since key management makes use of smart contracts, the certificate authority is the only organisation that is able to associate a public key with the actual identity of the person it corresponds to. A key revocation may be shown with the assistance of the smart contract recording key materials, which eliminates the need for a trusted centre.

II. REVIEW OF RELATED LITERATURE

Over the course of the last several years, a variety of information security for smart grids including edge computing systems have been developed. For instance, Tsai and Lo presented a system for anonymously access control that made use of psyche signing and encryption [13]. This would allow for the establishment of encrypted messaging connections. In addition, he and his colleagues introduced a novel authentication and key agreement system [14], which, in comparison to [13], had lower costs associated with both computation and communication. However, it was later discovered that the protocol is susceptible to the leaking of ephemeral secret keys and does not achieve the privacy of smart metre credentials. As a result, a better secured key agreement protocol was introduced [15]. Kumar et al. suggested a lightweight anonymously authentication and key arrangement technique [16] more recently in 2018. [16]

Using symmetric encryption, their method accomplishes the goal of achieving identity anonymity; thus, the neighbourhood area network gateway has to keep track of a number of different symmetric keys for the several home area network gateways. In order to facilitate real-time data flow, Chaudhary et al. suggested a software defined network (SDN)-enabled multifactor authentication for encrypted communication in a smart grid context. This was done in order to protect sensitive information. The peer entities are capable of communicating among themselves due to the use of a third-party authenticator known as Kerberos. The essential element encryption approach [17] ensures the confidentiality of the data while it is being sent. Following that, Chaudhary and colleagues [18] introduced a honeycomb method of key exchange that made use of a third party auditor. This new approach offers increased safety as well as more efficient when compared to the previous one [17].

Gope and Sikdar's suggested authenticated key cooperation protocol [19] included physically uncloneable functions (PUFs), and the two researchers also devised another inexpensive authenticating industrial wireless sensor network utilising

PUF [20]. A four different secure authentication technique that enables dynamic addition, password and biometric updating, and conventional anonymity was developed by Wazid et al. [21]. This protocol was designed for use with smart metres. Furthermore, the protocol does not provide flexible revocation, therefore it is not possible to delete or exclude smart metres that are malicious or malfunctioning. An efficient authentication technique for smart grid was presented by Mahmood et al. [22], however their approach does not enable anonymity since the true identity of smart metres is broadcast over the open channel in wireless networks. After then, Mahmood et al. introduced yet another anonymous key agreement mechanism for the edge computing architecture of smart grids [11]. Unfortunately, we discovered that the protocol does not accomplish authentication mechanism since the smart metre does not check the validity of utility control (that is, the value of Qi = 1 b+Ri Sj is not confirmed). This is the main reason why the protocol fails to achieve authentication mechanism.

Jia et al. designed and explicitly established the security of an identity-based anonymous authentication system for mobile edge computing [12] in the year 2019, and they did so in 2019.

Nevertheless, the protocol does not take into account the key management of the participants in the communication. A key management and authentication technique was presented by Kahvazadeh et al. for the edgecloud computing paradigm [23]. All devices, rather than authenticating with the centralised cloud, authenticate to a control-area unit that has been granted authorization (CAU). The cloud and the CAU are given the benefit of the doubt in this approach, and the devices are not responsible for determining whether or not they are legitimate. In addition, the protocol does not provide device anonymity or revocation, which reduces the usefulness of the protocol inside a smart grid environment.

An internal audit anonymity routing protocol using linkable group signature was proposed by Zheng et al. They also used blind signature, trapdoor indicative commitment, and signature of knowledge in the protocol [24]. The goal of this protocol was to provide provisional anonymity but instead dynamic participation. [25] Li and Cheng presented a technique for protecting users' privacy while using mobile sensing that was based on the region-based group signature. [26] Zhao et al. came up with a mechanism for protecting users' privacy while using trustworthy smart metres. The technique makes use of attribute certificates and ring signatures.

On the other hand, it is well knowledge that both group signature and ring signature systems take a significant amount of time to complete. Using pseudonyms as the basis for the cryptography, Amore et al. presented an authentication protocol for an edge-fog computing architecture that would protect users' privacy [10]. The protocol is successful in achieving secure key agreement while maintaining identity secrecy against fog servers; nevertheless, it does not prevent external assaults from being traceable. Moreover, if an end user moves away from his or her registration area, the authentication here between average consumer and a fog server needs to rely on an online RA, and that each cloud provider needs to maintain a verification list (called SV in [10]) to record the valid pseudonym identities. This is because the digital signature with

an end consumer and a cloud cover server is a two-way process. To put it another way, the communication costs associated with updating the list may be rather expensive, and the system is susceptible to attacks with stolen verifiers.

Therefore, coming up with anonymous authentication and key agreement techniques that are both reliable and secure for edge programming smart grid systems continues to be a challenge.

III. EVALUATION AND COMPARISON

We compare the effectiveness of the protocol that we have presented with those that have been developed by Amor et al. [10], Mahmood et al. [11], and Jia et al. [12].

Since Jia et al. [12] have assessed the effectiveness of some cryptographic algorithms used in the communication protocol here on Application Virtualization under Ubuntu system and using a Google Nexus Each smart phone to replicate the authority of endpoint and end user respectively, we will straightforwardly use their variables again for comparing. This is because Jia et al. [12] have assessed the efficiency of some cryptographic operations employed in the communication protocol on the Alibaba Cloud under Ubuntu system. The outcomes of their research are summarised in Table II. Due to the fact because they have a minimal impact on the overall performance of the system, the runtime of certain lightweight processes and the performance assessment of the registration phase are not included. The following chart provides a graphic representation of a comparative review of the calculation costs and communications expenses for our protocol, as well as the 3 protocols [11], [12], and [10].

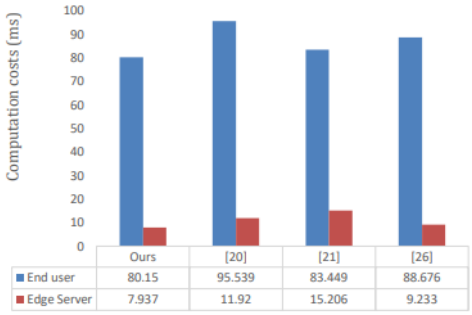

Figure 1 is a comparative overview of the computing and communication expenses associated with authenticating users.

To evaluate the operations of smart contract, we use the hyperledger-composer to build a permissioned test chain, where the version of composer is V0.20.7. The blockchain runs on the x86_64 GNU/Linux system with 1 core and 2GB RAM. With the Docker Engine, there are four permissioned nodes in the blockchain network, i.e., Fabric CA, Orderer, Committer and Endorser. The runtime of Algorithms 2 to 4 as shown in Table IV. Note that the running time is the sum total of the time for transaction issuing, verifying and synchronization. From Fig 2, we know that both computation and communication costs of our proposed protocol are the least for the basic cryptographic operations. And in our protocol, it needs only one round to exchange messages for mutual authentication, but the protocol in [10] needs three rounds of message exchanges for authentication and the protocol in [11] needs two rounds of message exchange. Note that if an end user wants to

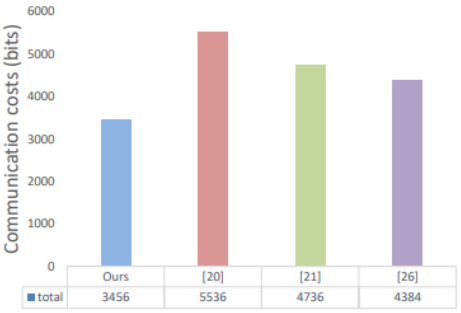

Figure 2 shows a comparison of the expenses of communicating for authentication

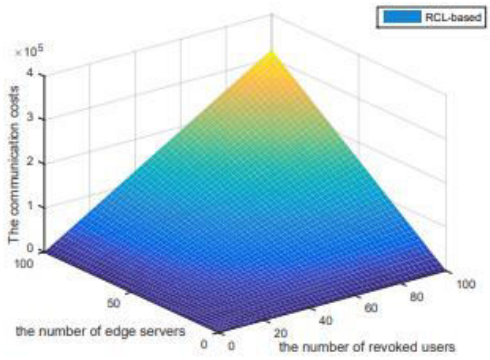

Figure 3: Costs of communication for revocations based on CRL data (B)

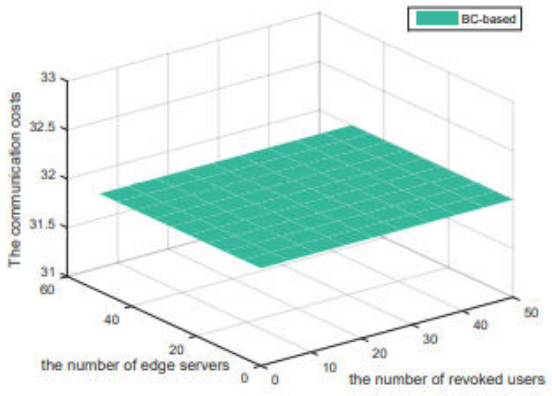

Figure 4: Costs of communication for revocations based in British Columbia (B)

communicate with such an edge node that is located in a different part of the network than its registered field, the communications costs associated with protocol [10]. In addition, the cost of maintaining these different necessities for end users is greater than the cost of updating them using our suggested protocol. This is because the protocol described in [10] needs to update all verifier lists that are supplied to the edge servers that are relevant to them.

When something came to the revocation, the authenticating time cost at the edge server's side might be as high as 234.233 milliseconds (ms), given that the cost of querying the blockchain is 0.225 seconds. Even if it seems to be a bit higher, it is still viable for a smart grid system. This is because a genuine edge server should have far more compute resources than our simulation platform has.

In addition, there are no extra expenses associated with calculation on the part of the end user when conditionally incognito is being supported. We do not compare the calculation speed on revocation here since the other protocols do not offer dynamic revocation. The telecommunication costs associated with revoking a certificate via the CRL are shown in Figure 4. We are able to observe that the expenses are going to skyrocket as the number of people who have their access revoked and the number of edge servers increases. However, it is clear that the communication costs of blockchain-based temporary suspension in our suggested technique are a constant number (i.e., the length of PID), given that it only needs to invoke the smart contract revokeKMST(P ID) given a parameter P ID, as shown in Fig.4. This is because it only needs to revoke this same consensus protocol when it is given a parameter P ID.

Because of this, while taking into consideration both safety and effectiveness, the protocol that we have presented is better suited for demand response systems that are based on edge of the network.

IV. CONCLUSION

In some kind of a power system architecture based on geometric computing, the ability to create confidential and safe communication between end users and edge servers is essential. In this article, an innovative system for anonymous authentication and key agreement that also features economical key management was introduced. In contrast to the majority of currently used protocols, such as those developed by Amor et al. [10], Mahmood et al. [11], and Jia et al. [12], the proposed protocol not only manages to achieve additional significant security properties in addition to the fundamental ones (i.e., mutual authorization, encryption information agreement, and replay attacks), but it also provides the fundamental ones (i.e., secure key agreement). The most notable aspect of this protocol is that it allows for quick key update as well as revocation while reducing the costs associated with communication. Additionally, it introducing financial identification anonymity while reducing the costs associated with computing. The findings of the performance assessment further reveal that the suggested protocol is even more efficient than the ones provided by Amor et al. [10], Mahmood et al. [11], and Jia et al. [12], while still meeting the required security features.

REFERENCES

[1] L. Lyu, K. Nandakumar, B. I. P. Rubinstein, J. Jin, J. Bedo, and M. Palaniswami, "PPFA: privacy preserving fog-enabled aggregation in smart grid," IEEE Trans. Industrial Informatics, vol. 14, no. 8, pp. 3733–3744, 2018. [Online]. Available: https://doi.org/10.1109/TII.2018.2803782

[2] K. Kaur, S. Garg, G. S. Aujla, N. Kumar, J. J. P. C. Rodrigues, and M. Guizani, "Edge computing in the industrial internet of things environment: Software-defined-networks-based edge-cloud interplay," IEEE Communications Magazine, vol. 56, no. 2, pp. 44–51, 2018. [Online]. Available: https://doi.org/10.1109/MCOM.2018.1700622

[3] S. Sarkar, S. Chatterjee, and S. Misra, "Assessment of the suitability of fog computing in the context of internet of things," IEEE Trans. Cloud Computing, vol. 6, no. 1, pp. 46–59, 2018. [Online]. Available: https://doi.org/10.1109/TCC.2015.2485206

[4] N. Kumar, S. Zeadally, and J. J. P. C. Rodrigues, "Vehicular delay-tolerant networks for smart grid data management using mobile edge computing," IEEE Communications Magazine, vol. 54, no. 10, pp. 60–66, 2016. [Online]. Available: https://doi.org/10.1109/MCOM.2016.7588230

[5] L. Wu, J. Wang, K. R. Choo, and D. He, "Secure key agreement and key protection for mobile device user authentication," IEEE Trans. Information Forensics and Security, vol. 14, no. 2, pp. 319–330, 2019. [Online]. Available: https://doi.org/10.1109/TIFS.2018.2850299

[6] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," IEEE Communications Magazine, vol. 56, no. 7, pp. 82–88, 2018.

[7] M. Badra and S. Zeadally, "Design and performance analysis of a virtual ring architecture for smart grid privacy," IEEE Trans. Information Forensics and Security, vol. 9, no. 2, pp. 321–329, 2014. [Online]. Available: https://doi.org/10.1109/TIFS.2013.2296441

[8] Y. Gong, Y. Cai, Y. Guo, and Y. Fang, "A privacy-preserving scheme for incentive-based demand response in the smart grid," IEEE Trans. Smart Grid, vol. 7, no. 3, pp. 1304–1313, 2016. [Online]. Available: https://doi.org/10.1109/TSG.2015.2412091

[9] K. Rabieh, M. M. E. A. Mahmoud, K. Akkaya, and S. Tonyali, "Scalable certificate revocation schemes for smart grid AMI networks using bloom filters," IEEE Trans. Dependable Sec. Comput., vol. 14, no. 4, pp. 420–432, 2017. [Online]. Available: https://doi.org/10.1109/ TDSC.2015.2467385.

[10] A. B. Amor, M. Abid, and A. Meddeb, "A privacy-preserving authentication scheme in an edge-fog environment," in 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA). IEEE, 2017, pp. 1225–1231.

[11] K. Mahmood, X. Li, S. A. Chaudhry, H. Naqvi, S. Kumari, A. K. Sangaiah, and J. J. P. C. Rodrigues, "Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure," Future Generation Comp. Syst., vol. 88, pp. 491–500, 2018. [Online]. Available: https://doi.org/10.1016/j.future.2018.06.004

[12] X. Jia, D. He, N. Kumar, and K.-K. R. Choo, "A provably secure and efficient identity-based anonymous authentication scheme for mobile edge computing," IEEE Systems Journal, 2019.

[13] J. Tsai and N. Lo, "Secure anonymous key distribution scheme for smart grid," IEEE Trans. Smart Grid, vol. 7, no. 2, pp. 906–914, 2016. [Online]. Available: https://doi.org/10.1109/TSG.2015.2440658

[14] D. He, H. Wang, M. K. Khan, and L. Wang, "Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography," IET Communications, vol. 10, no. 14, pp. 1795–1802, 2016. [Online]. Available: https://doi.org/10.1049/iet-com.2016.0091

[15] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," IEEE Trans. Smart Grid, vol. 9, no. 3, pp. 1900–1910, 2018. [Online]. Available: https://doi.org/10.1109/TSG.2016.2602282

[16] P. Kumar, A. Gurtov, M. Sain, A. Martin, and P. H. Ha, "Lightweight authentication and key agreement for smart metering in smart energy networks," IEEE Transactions on Smart Grid, 2018.

[17] R. Chaudhary, G. S. Aujla, S. Garg, N. Kumar, and J. J. P. C. Rodrigues, "Sdn-enabled multi-attribute-based secure communication for smart grid in iiot environment," IEEE Trans. Industrial Informatics, vol. 14, no. 6, pp. 2629–2640, 2018. [Online]. Available: https: //doi.org/10.1109/TII.2018.2789442

[18] R. Chaudhary, G. S. Aujla, N. Kumar, A. K. Das, N. Saxena, and J. J. P. C. Rodrigues, "Lacsys: Lattice-based cryptosystem for secure communication in smart grid environment," in 2018 IEEE International Conference on Communications, ICC 2018, Kansas City, MO, USA, May 20-24, 2018, 2018, pp. 1–6. [Online]. Available: https://doi.org/10.1109/ICC.2018.8422406

[19] P. Gope and B. Sikdar, "Privacy-aware authenticated key agreement scheme for secure smart grid communication," IEEE Transactions on Smart Grid, 2018.

[20] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks," IEEE Transactions on Industrial Informatics, 2019.

[21] M. Wazid, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "Secure three-factor user authentication scheme for renewable-energybased smart grid environment," IEEE Trans. Industrial Informatics, vol. 13, no. 6, pp. 3144–3153, 2017. [Online]. Available: https: //doi.org/10.1109/TII.2017.2732999

[22] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication," Future Generation Comp. Syst., vol. 81, pp. 557–565, 2018. [Online]. Available: https://doi.org/10.1016/j.future.2017.05.002

[23] S. Kahvazadeh, X. Masip-Bruin, R. Diaz, E. Marín-Tordera, A. Jurnet, and J. Garcia, "Towards an efficient key management and authentication strategy for combined fog-to-cloud continuum systems," in 3rd Cloudification of the Internet of Things, CIoT 2018, Paris, France, July 2-4, 2018, 2018, pp. 1–7. [Online]. Available: https://doi.org/10.1109/ CIOT.2018.8627111

[24] H. Zheng, Q. Wu, B. Qin, L. Zhong, S. He, and J. Liu, "Linkable group signature for auditing anonymous communication," in Australasian Conference on Information Security and Privacy. Springer, 2018, pp. 304–321.

[25] L. Ma, X. Liu, Q. Pei, and Y. Xiang, "Privacy-preserving reputation management for edge computing enhanced mobile crowdsensing," IEEE Transactions on Services Computing, 2018.

[26] J. Zhao, J. Liu, Z. Qin, and K. Ren, "Privacy protection scheme based on remote anonymous attestation for trusted smart meters," IEEE Transactions on Smart Grid, vol. 9, no. 4, pp. 3313–3320, 2018.

[27] C. Lin, D. He, X. Huang, K.-K. R. Choo, and A. V. Vasilakos, "Bsein: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," Journal of Network and Computer Applications, vol. 116, no. 1, pp. 42–52, 2018.

[28] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," Journal of Network and Computer Applications, vol. 126, no. 1, pp. 45–58, 2019.

[29] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," Ieee Access, vol. 4, pp. 2292–2303, 2016.

[30] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identitybased conditional privacy-preserving authentication scheme for vehicular ad hoc networks," IEEE Transactions on Information Forensics and Security, vol. 10, no. 12, pp. 2681–2691, 2015.

[31] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," IEEE Systems Journal, vol. 9, no. 3, pp. 816–823, 2015.

[32] D. He, Y. Zhang, D. Wang, and K. K. R. Choo, "Efficient and secure two-party signing protocol for the identity-based signature scheme in the ieee p1363 standard for public key cryptography," IEEE Transactions on Dependable and Secure Computing, pp. 1–10, 2018, dOI: 10.1109/TDSC.2018.2857775.

[33] Q. Feng, D. He, S. Zeadally, N. Kumar, and K. Liang, "Ideal latticebased anonymous authentication protocol for mobile devices," IEEE Systems Journal, pp. 1–11, 2018, dOI: 10.1109/JSYST.2018.2851295.

[34] T.-H. Lin, C.-C. Lee, and C.-H. Chang, "Wsn integrated authentication schemes based on internet of things," Journal of Internet Technology, vol. 19, no. 4, pp. 1043–1053, 2018.

[35] C. Meshram, C.-C. Lee, S. G. Meshram, and C.-T. Li, "An efficient id-based cryptographic transformation model for extended chaotic-mapbased cryptosystem," Soft Computing, vol. 23, no. 16, pp. 6937–6946, 2019.

Author Details

Dr. A. Avani obtained M. Tech degree from JNTU, Hyderabad, India. She is at present working as professor in Department of CSE of Anu Bose Institute

of Technology, Paloncha, Telangana, India. Her area of interest is Data mining.