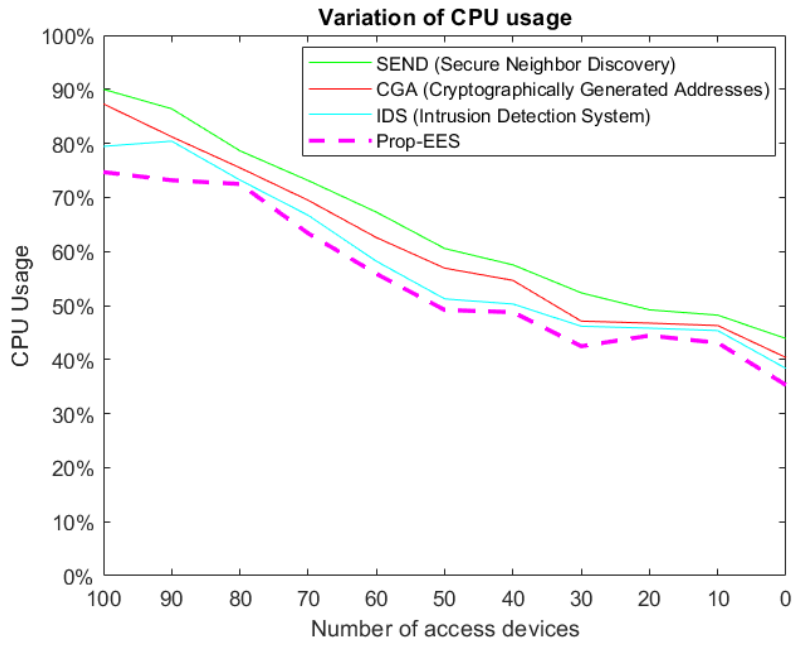

Fig.6. CPU Usage Vs. Number of Access Devices using SEND, CGA, IDS, MAPSDN-EESC

It is observed in the performance graph of the CPU usage versus the number of access devices that the utilization of the CPU in % trend is decreasing with respect to the increasing number of access devices for all the authentication protocols. Out of all the existing methods, i.e., SEND, CGA and IDS, the best performance is given by IDS, and the worst among these three is given by SEND, and the proposed authentication protocol MAPSDN-EESC outperform in respect to all. The table 4, tabulates the observation for a context of a network deployment with SDN, where the network utilization in % is taken as an independent variable, and the Authentication delay is a dependent variable measured in millisecond (ms) for the four respective methods of authentication which includes, SEND, CGA, IDS, and the proposed method MAPSDN-EESC.

Table 4.Authentication Delay in (ms) with corresponding Network utilization

Authentication delay in (milliseconds: ms)				
Network utilization (%)	SEND	CGA	IDS	MAPSDN-EESC
10	3.212	3.469	3.746	4.008
20	3.244	3.568	3.925	4.082
30	3.406	3.713	3.898	3.976
40	3.61	3.827	4.018	4.219
50	3.791	4.018	4.059	4.383
60	3.839	4.135	4.259	4.643
70	4.212	4.338	4.555	4.483
80	4.633	5.05	5.201	5.722
90	4.772	4.867	5.257	5.572
100	5.201	5.462	5.68	5.794

The fig.7 illustrates the trend of the variation of the fast authentication delay by the nodes with the changing values of the network utilization for all the four authentication protocols.

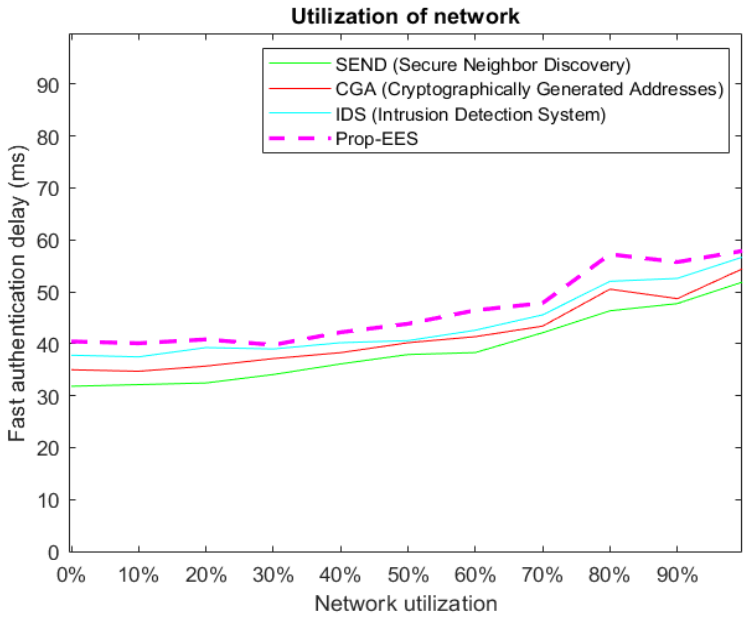

Fig.7.Authentication delay network utilization vs. number of access devices using sends, CGA, Ids, Mapsdn-Eesc

It is observed in the performance graph of the fast authentication delay versus network utilization that the fast authentication delay in ms, the trend is increasing with respect to increasing % of network utilization for all the authentication protocols. Out of all the existing methods, i.e., SEND, CGA and IDS, the best performance is given by IDS, and the worst among these three is given by SEND, and the proposed authentication protocol MAPSDN-EESC outperform in respect to all.

5. Conclusion

The fast adoption of the CPS and IoT works on the SDN based architecture for the more efficiency and flexibility because of the SDN supporting characteristics. The inclusion of SDN introduces much vulnerability that brings a huge security concern in the network. A strong security protocol relies on strong access control and authentication to protect the network from the resource access and data integrity. Many of the methods of authentication have certain limitations that do not support a large number of device authentication as well as poses higher computational complexities and dependencies on the trusted third party, which is exposed so some collusion attacks. To overcome these issues, this paper contributes designing an authentication scheme based on the recommended architecture of Trusted Computing Group Specification Architecture (TCGSA) to overcome large scale device application support and usage a light weighted key encryption based credential formation and its authentication process by the different operational units of SDN including DL, OFS, CV, COPLU, IVU, and AU. The analytical model is evaluated with the different key-encryption processes like CGA, IDS, and SEND. The performance evaluation of the model with this entity or attribute encryption method is performed with the performance metrics like delay, network utilization, authentication delay, and CPU usage and found that proposed EES provides optimal performance with respect to the CGA, IDS, and CGA. In the future research plan, analytical modeling with different network evaluation is planned with or without SDN in the presence of the attack and non-attack condition to understand the better aspect of the domain.

References

[1] L-de-Ipiña, D.; Chen, L.; Mitton, N. (2017): Ubiquitous Intelligence and computing for enabling a smarter world, PersUbiquitComput, 21, pp. 407–409

[2] Awoyemi, B.S.; Alfa, A.S and Maharaj, B.T.J.(2020): Resource Optimisation in 5G and Internet-of-Things Networking, Wireless PersCommun, 111, pp.2671–2702

[3] Abuarqoub, A.: A Review of the Control Plane Scalability Approaches in Software Defined Networking, Future Internet, 12(3), pp. 49

[4] Li, W.; Meng, W.; Kwok, L.F.(2016): A survey on OpenFlow-based Software Defined Networks: Security challenges and countermeasures, Journal of Network and Computer Applications, 68, 126-39

[5] S-Hayward, S.; Callaghan, G. O.; Sezer, S.(2013). SDN Security: A Survey, 2013 IEEE SDN for Future Networks and Services (SDN4FNS), Trento, pp. 1-7

[6] Alsmadi, I.; Xu, D.(2015). Security of software defined networks: A survey, Computers & security, 53, 79-108

[7] Akhunzada, A.; Ahmed, E.; Gani, A.; Khan, M. K.; Imran, M.; Guizani, S. (2015). Securing software defined networks: taxonomy, requirements, and open issues, in IEEE Communications Magazine, 53(4), pp. 36-44

[8] Shuangyu, H.; Jianwei, L.; Jian, M.; Jie, C.(2015). Hierarchical Solution for Access Control and Authentication in Software Defined Networks. In: Au M.H., Carminati B., Kuo CC.J. (eds) Network and System Security. NSS Lecture Notes in Computer Science, 8792

[9] Hongyu, Gao., Hu, J., Huang, Tuo., Wang, Jingnan and Chen, Yan.(2011). Security issues in online social networks. IEEE Internet Computing, 15, 4, pp.56-63

[10] Sahai, A.; Waters, B. (2005). Fuzzy identity-based encryption, In: Cramer, R. (ed.) EUROCRYPT, LNCS, Springer, Heidelberg, 3494, 457–473

[11] Wang, G.; Liu, Q.; Wu, J.(2011). Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers, Computers & security, 30(5), 320–331

[12] Wan, Z.; Liu, J.; Deng, R.H.(2012). HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing, IEEE Transactions on Information Forensics and Security, 7(2), 743–754

[13] Liu, J.; Lai, Y.; Diao, Z.; Chen, Y.(2017). A trusted access method in software-defined network, Simulation Modelling Practice and Theory, 1 (74), 28-45

[14] Arthur, W.; Challener, D.(2015). A Practical Guide to TPM 2.0: Using the Trusted Platform Module in the New Age of Security, Apress

[15] Lohstroh, M.; Kim, H.; Eidson, J.C.; Jerad, C.; Osyk, B.; Lee, E.A.(2019). On enabling technologies for the Internet of Important Things, IEEE Access, 25 (7), 27244-56

[16] Restuccia, F.; D'Oro, S and Melodia, T.(2018). Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking. in IEEE Internet of Things Journal, 5(6), pp. 4829-4842

[17] Singh, S.; Sharma, P. K.; Moon, S. Y.; and Park, J. H.(2017). Advanced Lightweight Encryption Algorithms for IoT Devices: Survey, Challenges and Solutions, Journal of Ambient Intelligence and Humanized Computing, pp. 1–18

[18] Cheng, H.; Liu, J.; Mao, J.; Wang, M.; Chen, J.; Bian, J.(2018). A compatible openflow platform for enabling security enhancement in SDN, Security and Communication Networks

[19] Ravindra, S.; Shankaraiah, S.(2020). Security and Authentication Scheme for Software Defined Network, International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, 9(4), 2020 [20] Sasaki, T.; Hatano, Y.; Sonoda, K.(2013). Load distribution of an OpenFlow controller for role- based network access control, Proc. of Network Operations and Management Symposium, Hiroshima, Japan, pp.1-6

[20] Mattos, D.M.F.; Duarte, C.M.B.(2016). AuthFlow: authentication and access control mechanism for software defined networking, Annals of Telecommunications,7, 607–615

[21] Raza, S. M.; Kim, D. S.; Shin, D and Choo, H.(2016). Leveraging proxy mobile IPv6 with SDN, In Journal of Communications and Networks, 18(3) 3, pp. 460-475

[22] Bernardos, C, J., Soto, I., Moreno, J.I. Telemaco Melia, Marco Liebsch, and Ralf Schmitz. (2005). Experimental evaluation of a handover optimization solution for multimedia applications in a mobile IPv6 network. European Transactions on Telecommunications, 16, 4, 317-328