MAPSDN-EESC: A MODELING OF AUTHENTICATION PROCESS FOR THE SOFTWARE DEFINED NETWORK USING ENCRYPTED ENTITY SCHEME CRYPTOGRAPHY

RAVINDRA S
Research Scholar, VTU, Belagavi, Karnataka, India
Email: ravindraa.s@gmail.com

Dr. Shankaraiah
Professor and Head, Department of Electronics and Communication,
SJCE, Mysuru, India

Abstract - The distinguishing characteristics of the SDN provide flexibility to build a robust ubiquitous application but also suffer various security challenges. The effective authentication process provides solutions towards mitigating the adverse effect on network performance and data protection. The typical limitations of the existing systems of authentication are not so scalable due to the higher complexity of flow rule monitoring. The proposed model of the authentication for the SDN uses the mechanism suggested by Trusted Computing Group Specification Architecture and encrypted entity cryptography as an evolution of attributed based encryption. The proposed method MAPSDN-EESC provides lightweight authentication mechanism along with the cross-platform validation of the legitimate user. The proposed method EES reduces the latency by 12.89%, 9.2%, and 4.9% as compared to the existing method of SEND, CGA, and IDS, respectively. The CPU usage reduces by 14.44%, 9.60%, and 4.91% as compared to the existing method of SEND, CGA, and IDS, respectively. The fast authentication delays are lower by 17.44%, 10.44%, and 5.12 % as compared to the existing method of SEND, CGA, and IDS, respectively.

Keywords: Authentication., Attribute-based Encryption., Network security., Software Define Network., Trusted Computing Group Introduction.

1. Introduction

Many of the advances are witnessed in the recent past in the ubiquitous and context-oriented application in various domains of smart and intelligent transport, factory, city, healthcare, etc., systems [1]. These advancements have become possible due to modern technologies of embedded systems, sensors, networks (WSN, IoT, MANET, CRN), and communication standards (4G-LTE, 5G)[2]. The core backbone of the network on which these applications rely on a core network component at the Layer-2(L2) and layer-3(L3) routers and switches capabilities. The inclusion of the software-defined network (SDN) is an advantageous against the traditional components at the L2/L3 because of the distinguishing characteristic of operating in a centralized manner with the partition or isolation of the different planes (such as data plane and the control plane). Due to this separation of the plane, it provides a higher capacity to manage the network traffic more effectively. Another advantage of the inclusion of SDN is the flexible reprogramming, and these characteristics make the SDN based system more flexible and robust [3]. The new layer and architecture of the SDN based application introduce associated vulnerabilities that provide an opportunity to the adversaries to plan attacks to gain the benefit by means of compromising the network operation as well as access to the data, many of such attacks are being reported in the literature[4][5][6].

Unlike the core characteristics of the security protocol designs for any network, even SDN also require to handles issues like authentication, integrity, access control, authorization, and non-repudiation along with proactive and reactive approaches to handle a defined attack pattern [7]. The effective authentication scheme mitigates many of the security challenges as well as complements another security requirement. The strong and effective authentication scheme controls the adversary or the intruder to gain access to the data as well also helps to protect malfunctions on the network operations from the manipulation by the attackers. The biggest vulnerability in SDN is the lack of a strong, consistent, and more effective authentication mechanism so that it can authenticate the stakeholder from the different layers of the network as well as application units. In lack of

DOI : 10.21817/indjcse/2020/v11i4/201104270

this, attackers easily gain access with less effort, and the entire network gets compromised and leads to data leakage.

Most of the studies in SDN orient towards the utility factor and efficiency, but security concerns are the barrier to the fast adoption of SDN in future generation network applications [8]. There are very few contributions found in literature towards the authentication or access control mechanism in SDN. The initial device access mechanism does not satisfy the security concerns of large-scale networks [9]. If all the network devices are provided with equal priority as found in the legacy schemes for access control, then the use of memory space becomes inconsistent. The applicability of existing protocols for authentication in the new architecture of SDN limits its scope as the SDN takes charge of authentication. The attribute-based encryption (ABE) [10], has gain popularity to design access control and authentication schemes. However, the ABE schemes suffer from the key escrow problem. The further evolutions in this regard are taken place with a layer-wise approach of encryption of attributes [11] and managing attributes in the recursive manner [12]. Still, it requires translation efforts form one domain to another domain, which poses higher computational overhead in large scale device authentication requirements.

The formation of a special interest group, namely Trusted Computing Group Specification Architecture (TCGSA), provides a baseline for Authentication, which advocates the use of keys certified or signed by the attestation identity key (AIK). The TCGSA supports for the unlimited identities authentication [13]. This paper proposes a modeling architecture of an authentication mechanism suitably for the SDN to achieve the goal of the level of security along with the optimization of computation and time complexities. The method uses the cryptographic approach of entity encryption as an evolution of traditional attribute-based encryption in accordance with the philosophy of TCGSA [14]. The method also handles the challenge of constraint access of cross-platform, where the legitimate user provides the correct credential from an untrusted or unauthenticated system.

The paper organization is section 2 contains the inferring of the related work, section 3 describes the system model and section 4 discusses the performance evaluation of the model followed by the conclusion in section 5.

2. Related Work

The Internet of Things (IoT) collaborates various sub-networks with different traffic patterns that require an optimal pattern management system. The SDN offers better management of the traffic pattern due to its system-wise time scaling mechanism; therefore, IoT uses SDN. However, the legacy vulnerabilities of SDN demands a suitable design of a robust authentication protocol for security and authentication in SDN enabled IoT. The use of certificate-based authentication is being advocated in [15]. The IoT is gaining popularity, so addressing the security issues are critical for its reliability. The use of the traditional approaches for security schemes and protocols limits its usability due to its static approach to operations. In contrast, IoT requires more proactive, dynamic, and adaptive security approaches. The use of artificial intelligence and SDN fulfills the requirement of inelegancy and reconfigurability. The suitably designed authentication scheme ensures to mitigate many of the ill effects of attacks. The traditional PKC based authentication is not suitable in the eco-system of SDN enabled IoT due to its computational overhead. Therefore, a significant number of works are witnessed in the literature that proposes lightweight encryption schemes for authentication [16-17].

The study towards the security of the access control of the SDN is found in the work of [18], the focus is on the security of the OpenFlow controller, where the authentication of each flow takes place before getting registered. But it not so flexible due to its limitations of re-programmability. An extensive survey on the security aspects is in [19].In the traditional network, the inter attack takes place mainly because of the infected devices or the colluded devices with malicious intension, which cannot be handled with the typical firewalls. In order to handle these kinds of attacks, [20] introduces an OpenFlow based access control mechanism using a role-based architecture. This role-based control mechanism suffers performance degradation in large device networks because it requires controlling all the traffics, whereas it reduces the dynamic rules to approximately 93%. The [21] proposes a host credential as a certificate-based authentication scheme, namely: “AuthFlow.” This scheme places the device authentication process on the top of the MAC layer in the OpenFlow network and works based on priority mapping. The device identity is considered for form flow rule. The scheme was validated on the POX controller, which ensures low overhead and refined access control; it is economically not feasible and complex to implement in real-time scenarios.

In case of heavy traffic including multimedia in mobile IPv6 suffers latency problem, to handle this issue in [22], an Open Flow proxy mobile for Ipv6 implements controller for the centralized access gateway by isolating control and the data path to support the device mobility and exploits the authentication information to reduce the latency.

3. System Model

The proposed analytical system model contains an integrated approach of network deployment, route discovery process by SDN – control plane, communication and authentication, usage of different key mechanisms like SEND, IDS, and CGA, and finally, their comparison with the proposed Encrypted Entity Scheme (EES). As the TCGSA recommends the inclusion of the trusted computing mechanism for the purposes of verifying the user's platform integrity while requesting access to the SDN enabled network. Therefore the efficiency of the user device verification improvises. However, the TCGSA based proposed EES authentication process is flexible because it is compatible with the existing platforms as well as future generation networks supported with the SDN.

3.1 Network Deployment or Setup

The deployment of **SDN** contains three distinguished units, namely control plane (**Cp**), application plane (**Ap**), and data plane (**Dp**), such that the SDN={Cp, AP, Dp}. The typical internet of Things, WSN, or any wireless networks adopt hop by hop communication consist of '**N**' number of nodes(**n**) or access devices (**Ad**), which are deployed in the monitoring region in the random manner, which forms a graph **G(V)**. In order to form G(V), for each node, the localization process is performed using a random number generator function: frand() and a primal factor (**Hp, Vp**) for uniform distribution. The localization for $\forall$**Nk**$\in$ N as [$\mathbf{n_x}$,$\mathbf{n_y}$] is computed using equation (1) and equation (2), respectively.

$$n_x = Hp \times frand(Ni) \text{ for } \forall\ 1 \le i \le N \quad (1)$$

$$n_y = Vp \times frand(Ni) \text{ for } \forall\ 1 \le i \le N \quad (2)$$

The combined architecture of the wireless network, along with SDN, is shown in fig.1.

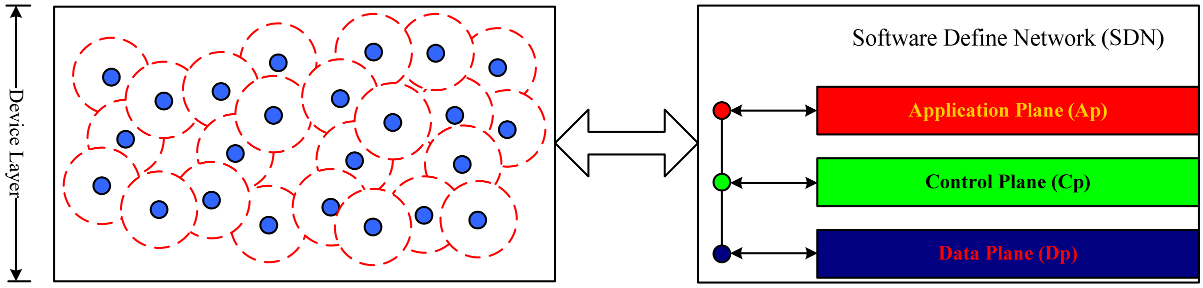

Fig.1. The architecture of the SDN enable wireless network

Each n$\in$N gets connected directly to the SDN; therefore, the G(V) updates as G(V, SDN). The pseudo algorithm for this is given below

Algorithm 1: Pseudo algorithm for network deployment

```
Input: N, Ap, Cp, Dp
Output:
Start:
SDN ← ={Cp,AP,Dp}
[$n_x$/ $n_y$]= (Hp / Vp) x frand(Ni) for $\forall$ 1≤i≤N
G(V, SDN) ← Graph
End.
```

3.2 SDN-Control Plane

Whenever a node ($\mathbf{n_i}$) as a sender wants to send data to the node ($\mathbf{n_j}$) as a destination, the control plane decides route by selecting the set of hopes as n_h = {n_{h1}, n_{h2}, n_{h3}…} depending upon the distribution of the node. This process of deciding intermediate hop nodes is known as route discovery.

Algorithm 2: Route discovery process at Control plane

```
Input:G(V, SDN), $n_x$/ $n_y$, $n_i$, $n_j$
Output: Route ($\vec{R}$)
Start:
        [$(n_i)_{x,y}$ , $(n_j)_{x,y}$] ← n(i , j)
Initiate route discovery process @ control plane:
                Initialize, R,Sxy,Dxy
                [$In_h$]← $\forall$ Ed($n_i$ , N-$n_i$) <R
                For each Inh compute $\vec{L}$ , Nr
                Nc←Ed(Nr)
                Sort(Ed(Nc))
                        Compute, Hn
                                Iteratively update the route: :[ $n_i$ , Hn, Nc]
                        Break; once $n_j$
Update:
($\vec{R}$)←[ $n_i$,Hn, $n_j$]
End.
```

The route discovery process (**RDP**) algorithms initially initialize the communication range(**R**) of the devices or nodes (n) assuming a uniform communication range for all the devices. The localization of the sender and the receiver nodes **Sxy**, **Dxy**$\in$ [n_x / n_y]. The system failures or any of the attacks introduce a fault in the established route that requires a route recovery process (**RRP**). The model counts of the total fault occurrence (**Ft**) in the RDP. The model MAPSDN-EESC considers total time taken in the routing process, including OpenFlow registration time with the control plane and the time to authenticate the devices. In order to find the neighbour node(n_h) and their index (**In**$_h$) for n_i the Ed(n_i , N-n_i) <R., where Ed is the Euclidean distance.

The link vector computation module computes for each node at the indices ‘Inh’ creates a link vector ($\vec{L}$) and the range node (Nr) so that the closet node (Nc) from the Nr is computed using (Ed) between the chosen node and the receiver. The sorting of $\forall$ the Ed of Nr takes place, then the next-hop (Hn) computation takes place. The final route (($\vec{R}$) merges iteratively as: [n_i,Hn, n_j] until the destination is achieved.

3.3 Communication and Authentication

The computed route ($\vec{R}$) as [Source Node→Hop→1-Hop→Hop-2→Hop-n→Destination Node] as [n_i→Hn_k, n_j], k is the number of hop nodes in ($\vec{R}$) gets registered in the open flow enables switch of SDN. The process of the proposed encrypted entity scheme (EES) based authentication is illustrated in fig.2.

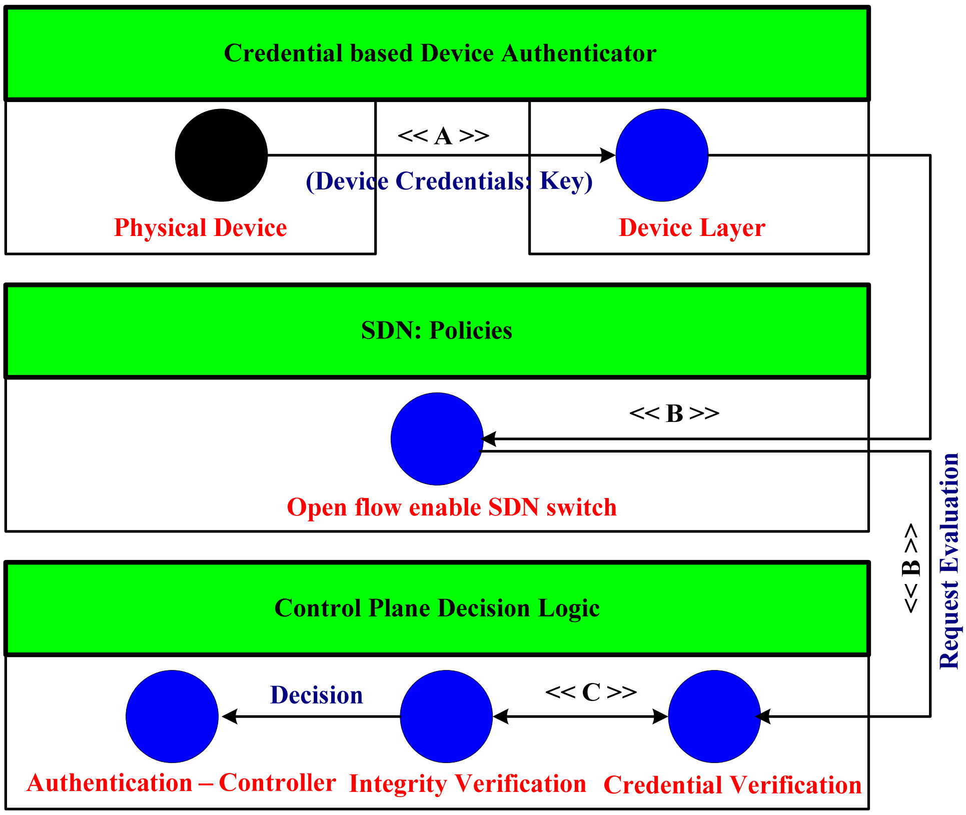
Credential based Device Authenticator
<< A >>
(Device Credentials: Key)
Physical Device
Device Layer
SDN: Policies
<< B >>
Open flow enable SDN switch
<< B >>
Request Evaluation
Control Plane Decision Logic
Decision
<< C >>
Authentication – Controller
Integrity Verification
Credential Verification

Fig.2. MAPSDN-EESC: Architecture of the Authentication process using an encryption scheme

The proposed TCGSA based authentication process supports for the multiple devices' authentication. The framework consists of a unit namely credential-based device authenticator (CDA), where every device as a node(n) communicates with the operation at the unit device layer (DL) for the registration process with their respective IDs and a key which is encrypted using entity encryption scheme (EES). The EES engine initially creates a pointer of all the characters (Ch) = {Alphabets, '.', Numeric, Special character}, further, it creates the randomly sampled data (Ds) = {S, NCh}, where NCh is the number of character elements and S =1 to NCh, without any replacement. The user can provide any keys, including alphanumeric and special symbols, which are filtered for shuffling. This process of shuffling makes it harder to guess by the attackers as well as this logic can be updated from time to time so that the compromise becomes further harder.

Ch ←*f*([q,'w',…'m,'n', Q, W…, B,N,M, 1,2,…9,0,…=, \ , @, #, $,…&, * ,…])

The input data for sampling takes a series 'S' and Nch as a number of samples for elements ∈ Ch to get the value of shuffled and chaotic arrangement of the elements of Ch, assigned into a vector: **Ph**. The key assigned to the devices as a node (n) is 'K' goes through a matching process between Ch and Ph, as shown in fig.3.

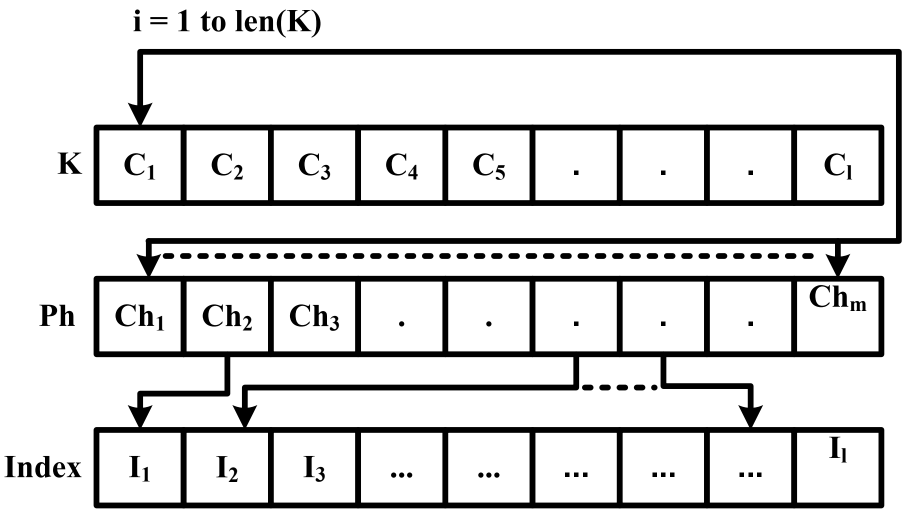

Fig.3. Match process between Ch and Ph

The process of encrypted key (Ek) takes the value of $j \in I$ $\forall$Ph, where j = 1 to length of 'I', s.t $Ek = Ph\ (I)_i \cup Ph\ (I)_j$; where i = 1, j = length of (I). The process of the EES is lighter in computation compared to SEND, CGA, and IDS method. Though the sequential time complexity to encrypt, the key is slightly higher in the simulation time, as listed in table I. the result is obtained by the profiling on the numerical computing platform.

Table.1. Sequential time of imitating the algorithm for Prop-EES, SEND, CGA and IDS

METHODS→	PROP-EES	SEND	IDS	CGA
TIME OF EXECUTION(S)	1.099	0.025	0.016	0.012

The wireless networks adopt an ad-hoc technology which enables the participating devices to auto-configure themselves after the address conflict and establishes the radio links among themselves to form the network. These distinguished behaviors of the devices and network become a vulnerability, which is exploited by the intruder or the attacker to implant their nodes programmed to participate in the route discovery and drop the packet strategically to degrade the performance of the network. The models are evaluated with the varying percentage of the attacker nodes or faulty nodes. Therefore the process of route discovery considers both healthy as well as faulty nodes in the route discovery process and data transmission.

The proposed EEC based authentication with the SDN ensures the elimination of such faulty nodes, so after the encryption process of the device credentials, the request from the DL goes to the SDN -policies unit, where the Open flow enabled SDN switch (OFS) send the request of evaluation for the credentials sent by the device through the DL to the credential verification (CV) unit of the control plane logic unit (CPLU). The CPLU verify the credentials then it sends the verified credential to another unit Integrity verifier (IVU) in the CPLU, where the IVU, check the integrity of the credentials and sends its decision to another unit namely authentication controller (AU) in the CPLU, which executes this decision while routing on the packet-in messages. The typical controller's functions during combine authentication and communications are a) Packet-in message sent to the controller, b) Listening packet in the message, c) extract neighbor discovery from the packet in, d) verifying identity of the packet from global information of network and then finally if faulty or attacker or malicious node identified: Unauthenticated node identified!. The fig.4 below illustrates the communication with the authentication process for a context of network deployment

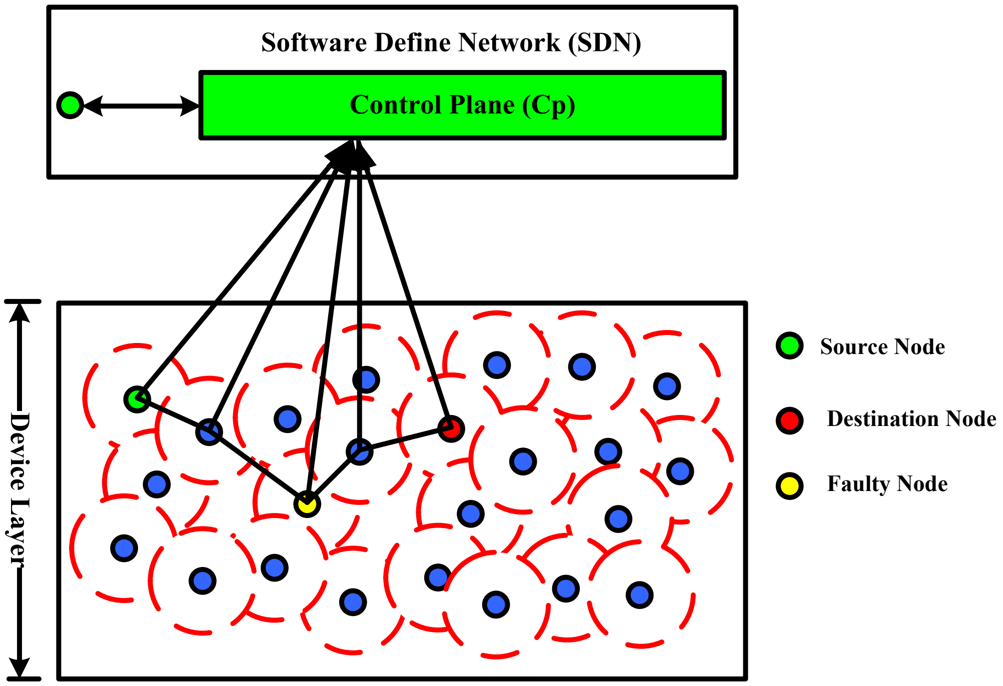

Fig.4. The communication process with EES based SDN controller Authentication process

The modified controller combinedly handles the integration of the device registry in the multi-dimension aspect of the function of the access control. In contrast with the certificate-based method the Prop, ECS works with lightweight, encrypted key verification in the conjunction of the SDB based controller for the permission on the traffic flow so that both the user identity and platform of usage both are authenticated as complying the vision of the baseline architecture of TCGSA to meet the large scale nods in the cyber-physical systems(CPS) and IoTs.

4. Result and Analysis

The evaluation of the proposed authentication model for the SDN enabled IoT system, or a wireless network is performed for Latency, CPU usage with the device or node deployment density. Another performance metrics is authentication delay with respect to the network utilization. Table 2 tabulates the observation for a context of a network deployment with SDN, where the number of devices is taken as an independent variable and the latency is a dependent variable measured in seconds for the four respective methods of authentication which includes, SEND, CGA, IDS and the proposed method MAPSDN-EESC.

Table.2. Latency in (second) with corresponding No of Access Device

Latency in (Seconds)				
No of Access Devices	SEND	CGA	IDS	MAPSDN-EESC
10	5.659	5.603	5.435	5
20	5.716	5.602	5.154	4.96
30	6.147	5.655	5.598	5.374
40	6.272	5.833	5.308	5.202
50	6.892	6.479	6.22	6.158
60	7.417	7.189	6.758	6.217

The fig.5 illustrates the trend of the variation of the delay introduced with the changing values of the number of devices for all the four authentication protocols.

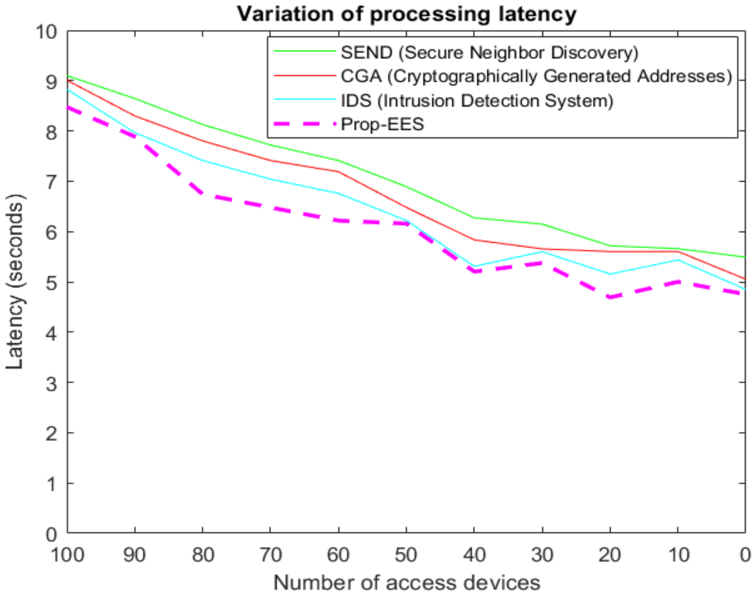

Fig.5. Latency Vs. Number of Access Devices using SEND, CGA, IDS, MAPSDN-EESC

It is observed in the performance graph of the Latency versus a number of access devices that the delay trend is decreasing with respect to 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.

Table 3 tabulates the observation for a context of a network deployment with SDN, where the number of devices is taken as an independent variable and the CPU usage is a dependent variable measured in % for the four respective methods of authentication which includes, SEND, CGA, IDS, and the proposed method MAPSDN-EESC.

Table.3. CPU Usage (second) with corresponding No of Access Device

CPU usage in (%)				
No of Access Devices	SEND	CGA	IDS	MAPSDN-EESC
10	4.822	4.629	4.536	4.309
20	4.92	4.674	4.58	4.443
30	5.234	4.711	4.616	4.247
40	5.752	5.464	5.027	4.876
50	6.054	5.691	5.122	4.917
60	6.727	6.256	5.818	5.586
70	7.312	6.946	6.669	6.335
80	7.862	7.548	7.321	7.248
90	8.64	8.122	8.04	7.317
100	9	8.73	7.944	7.468

The fig.6 illustrates the trend of the variation of the CPU usage by the nodes with the changing values of the number of devices for all the four authentication protocols.

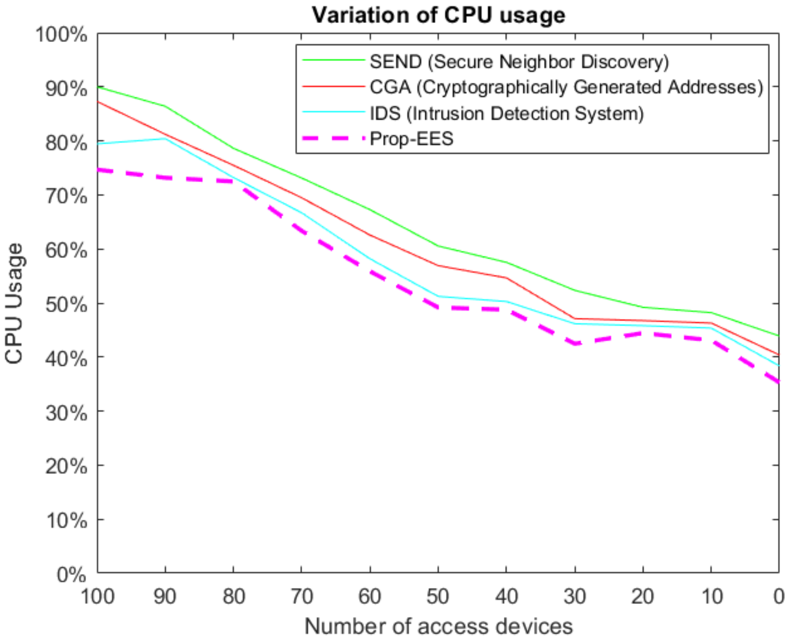

Fig.6. CPU Usage Vs. Number of Access Devices using SEND, CGA, IDS, MAPSDN-EESC

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.

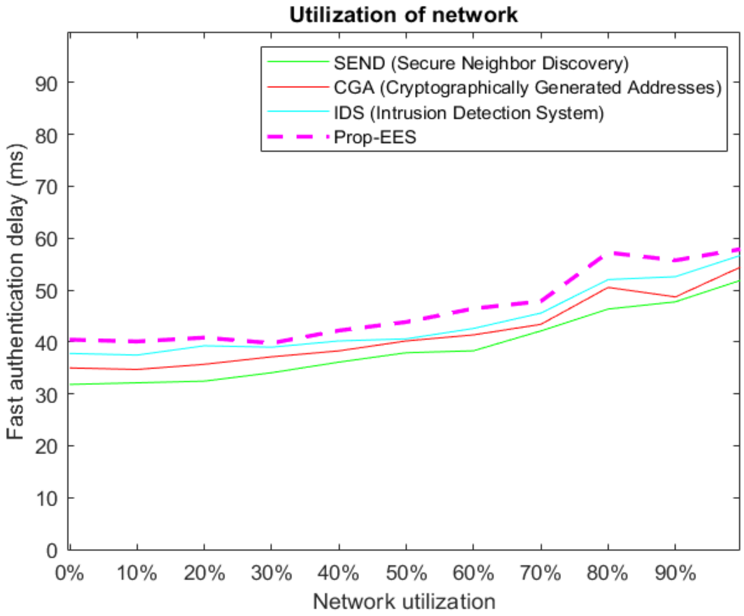

Fig.7.Authentication delay network utilization vs. number of access devices using sends, CGA, Ids, Mapsdn-Eesc

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