xIlkogretim Online - Elementary Education Online,2021; Vol 20 (Issue 1): pp.2447-2455
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.01.275

Types, Applications and Enhancements in Access Control

Vishaka Iyengar, Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Tamil Nadu, India
Brinda Bhowmick, Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Tamil Nadu, India
Sandeep Kumar P, Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Tamil Nadu, India

Abstract-Network Access Control broadly refers to the management of a network with respect to the devices/users that have access to it, and what they have access to. With networks serving as the backbone to all communication at various levels, be it in a private network or one owned by an organization, security of the resources that are accessible via this connection becomes increasingly important. Access control is a major aspect of this security. A powerful access control model inculcates/caters to the requirements of Confidentiality, Integrity and Accessibility. In this paper, we have surveyed the types of access control, network security and the latest schemes/protocols within it and the efficiency of these protocols. Any improvements or loopholes in the existing systems have been noted. Furthermore, we have reviewed the applications of access control in IoT systems.

Keywords: Network Access Control, IoT systems, private network.

I. Introduction

Network Access Control (NAC) is the act of managing the network. [1]It keeps unauthorized users and devices out of a private network and determines what data authorized users can access. This is necessary to maintain security compliance regulations [16]. Be it a private or a corporate network, the number of devices not nativetothenetworkareincreasing.Thus,itisimperativetoensureNetworkSecurity and access control. NAC is one aspect of Network Security. [3]Using various tools, schemes, algorithms and devices we can restrict not only the users that enter the network but also what they have access to. Furthermore, we can set up multi- factorauthenticationandalsomonitorthebehavioroftheдeviceswithinthenetwork. [4]A secure NAC system also ensures application security as a consequence of its additionalsecuritylayers.ThispaperisasurveyonNetworkAccessControlmechanisms with respect to confidentiality, integrity, accountability, authentication in compliance with the efficient utilization of the available resources.

Access control permits who can access a resource, under what circumstances and what they can do with that resource[14] [William Stallings 6th edition - cryptography and networksecurity].AsuccessfulAccessControlmodelensuresconfidentiality,integrity and availability. It’s types - attribute-based, certificateless, role-based and task-role based access control [5] are a few sought out mechanisms, which have been concentrated on.

We then consider network security and the CIA triad, which is its foundation [18]. Within network security, we delve into schemes such as Accountable and Privacy Enhanced Access Control (APAC), Token -Constrained permission delegation Algorithm (TCPDA), and LiCo. We then consider improvisedmechanisms for security and ways to increase their efficiency. Lastly, we study a few IoT based applications where access control plays a major role [12].

II State ofArt

A Access Control

Access control plays a major role in securing data in modern-day systems. [11]It controls who can access a resource, under what conditions and what they are permitted to do whilstaccessingtheresources.Userauthenticationformsthebasisforaccesscontrol and ultimately User accountability [13]. This is done by evaluating login credentials usingpasswords,biometricscans,PINs,securitytokensetc.Majorityofthechallenges in access control occur because of the highly diversified and dynamic nature of systemspresentinthenetwork.Tracingandtrackingassetsthatarebothlogicallyand geographically spaced poses further challenges. A nifty access control technique should all the security requirements to achieve Confidentiality, Availability and Integrity. [17] Its typesare:

B Attribute-Based Access Control

Access management using attributes is primarily used for IoT environments by the employment of blockchain technology against single-point failure and data tampering[19] byrecordingthedistributionofattributes.Furthermore,optimizationoftheprocesshas been done to achieve greater efficacy for IoT devices, hence withstanding several attacks efficiently.

The issue of robustness and trust is dealt with the scalable and decentralizedaccess control mechanism.[17]The attributes' authorization is recorded by adopting a new type of arrangement. The IoT devices referred to in this system are separate to the concurrence process of the blockchain network that greatly reduces the overall computation and communication overhead. [2]The scheme empowers fortifying the adaptabilityoftheframeworkandimprovesupkeep.Uponanalysisandsimulation,the scheme proves to provide secure, efficient and effective accesscontrol.

C Certificateless AccessControl

Wireless Body Area Networks (WBANs) are widely used in health monitoring applications. This implies selective access to medical data. This paper proposes an efficient certificateless sign-cryption and access control scheme which achieves Privacy,Integrity,Authentication,PublicVerification,Non-repudiation,andAuthenticity ofCiphertext.

In examination with three existing access control schemes, this strategy is best as far as computational expense and energy utilization for the controller.

Theadvantageofcertificatelesscryptography(CLC)isthatitdoesnothavepublickey certificates or the key escrow problem. This scheme still requires a trusted third party called the Key generation Centre (KGC) to create a partial private key which is subsequently combined with the user's secret key to form the full private key.Identity- based sign-cryption is capable of authenticating the clients while safeguarding the query messages. However, as it is based on IBC it has a key escrowweakness [16].

Shortcomings of previous schemes include:

1. The requirement of public-key certificates, without which key escrow problem arises.
2. The ciphertext is not authenticated directly. The ciphertext must be decrypted toascertainitsvalidityfailingwhichthedecryptionprocessbecomesineffective. [20]This process has the following merits over the previously researched schemes.
3. Thisschemedoesn'trequirepublickeycertificatesorhavekeyescrowproblem.
4. The controller can validate the ciphertext without decryption.[4]

D Role-Based AccessControl

RBAC is a highly preferred access control model for numerous reasons. RBAC restricts the access of information to people based on their roles. [15]Information is accessible as per the requirement. Hence, several constraints are implemented with respect to theoretical and practical considerations.

ThemeritofRBACisthatinorganizationswithlargenumbersofusersandresources, managing the permission delegation becomes easier and flexible. [13]However, the valuation of converting to an RBAC architecture from a traditional one is high. There are two methods by which we can configure RBAC - top-down and bottom-up approach.

Experts examine the entire company structure, relationships and needs of individuals at all levels in the top-down approach, and then atomize the activities into more manageable segments that share the same authorization arrangement.Data mining algorithms are used in the bottom-up approach to determine the roles and requirements specific to every organization.This paper focuses on techniques to improve previous proposals. [14]

E Task-Role-Based AccessControl

Complexity and dynamic nature of strategies formulated for access control ledto challenges in monitoring. The current access control models are static. They lack DynamicSegregationofDuties(SoD),TaskinstancelevelofSegregationanddecision making inreal-time.

Existingsolutionsareusedtodevelopamodel.ItcombinesthedynamicSoDtoensure access monitoring and liability on a whole. It strengthens prior access control techniques which include RBAC by dynamically permitting rights of user access. [7]Augmentation of the XACML policy language OASIS standard to support access needsintermsofdynamicconsiderationsandimplementtheaccesscontrolprotocols for decision making in real-time and to combat threats with respect to access control. The outcomes show that the model is measurably consuming multiple complex requests and can meet the requirements of dynamic access control.[5]

F Network Security

Network Security generally deals with two broad issues - Data security and Network System security. While data security deals with protecting the confidentiality of the data, network system security focuses on illegal attacks and maintaining the availability and integrity of the data. Together they form the CIA triad of security [18]. The CIA triad can be explained as follows:

Confidentiality (C) - Only authenticated parties can access the data meant for them. [19]
Integrity (I) - This can be further divided into 2 parts:
System integrity - The system untampered/modified in any way shape or form.
Data integrity - The information is changed only by authorized users in a specified manner.
Availability (A) - The data is always available. Though the topic is diverse, we have studied selected aspects of it. [22]
Additional factors in network security are:
Authenticity - The source can be verified to be who they say they are and that theyare genuine.
Accountability - The actions of an entity should be traceable back to that unique entity. This includes Non-repudiation, Deterrence, fault isolation, intrusion detection, prevention and after recovery. [22]
Within the topic of Network Security, we have looked into the following research that was conducted.

G Apac Scheme

Accountable and Privacy Enhanced Access Control (APAC) is a scheme that focuses onimprovingthesecurityintermsofconfidentialityofuserdataandholdingmalicious usersaccountablefortheiractions.ThisisdonebygettingridoftheTrustedThird-partysystem and introducing a scheme where any user in a group can anonymously generate the key. However, the entire scheme is based on the assumption that the systemparametersforthesignaturearehonestlygeneratedbyafullytrustedparty.

Aswedonothaveafullytrusted3rdparty,wesplitthisworkbetween2entitiescalled LawAuthorityandNetworkOwner.Ifeitherofthesepeopledoesnothonestlygenerate the parameters, then it's easy for them to find out who created the Group Signature and the safety provided by the APAC fails.[1]

H Tcpda Scheme

In a network, [2] permission is delegated or assigned to individuals based on the resource and task requirements. However, due to the inconsistency of the owner and manager of the resource unauthorized access may occur. In an IoT system, thereare many suchinconsistencies.

The Token -Constrained permission delegation Algorithm (TCPDA) scheme transforms the access control policy based on the constraints they must correspond to and embeds them into the permission token. Furthermore, there are additional constraints placed on the permission token to prevent them from being transferred or shared to unauthorized users. [10]Thus, only the users that meet the parameters can receive the tokens which solve the Unauthorized Access Vulnerability problem. Generally, a centralized decision-making system employing a trusted third party is in place. However, research suggests that these trusted systems are often not so trustworthy. Thus, this system is replaced with a blockchain. Since the blockchain is maintained by multiple institutions, trust can be established. Also, the invariable and traceable attributes of the blockchain address the issue of tracking information leakage.

I LICO

In an Operating System, various processes have varied privileges to access different resources. Due to inter-networking, which can occur iteratively, the monitoring of inappropriately accessed privileges becomes difficult.[15]

Inter-invoking occurs when processes interact frequently with each other. While each process has distinct or separate privileges, security vulnerabilities may arise when inter-invokingtakesplace.[11]Problemsfurtherarisewhenprivilegeregulationisdoneby a switch in a binary format. This process might create loopholes for privileges to be assigned to processes that should not getit.

The proposal is a design for a generalized access control mechanism that can be extended to schemas including social networking. It aims to introduce a lightweightdirected graph-based model, LiCo, which is modelled to achieve authorization of privileges amongst processes that are inter-networked. LiCo is programmed to effectively recognize collisions amongst privileges, raise an alarm and authorize the correctprivilegesproperly.[9]ThecostofthismodelisonlyO(n),wherenistheaccessor vertex number in the access controlgraph.

III IMPROVISED MECHANISMS FOR EFFICIENCY AND SECURITYIMPLEMENTATION

A Data Aggregation

A wireless sensor network (WSN) comprises of parent nodes and their subsequent nodes that communicate and accumulate data at the node corresponding to the base station. Due to its cost-effective implementation, WSNs are used in diverse applications that include healthcare, monitoring military surveillance, homeland security etc. [6]

The distributed wireless attribute of WSN makes it prone to various data breach and attacks which results in data loss and delay. An attacker can easily manipulate the links within a network and due to high sensitivity of data in WSN. Hence, the implementation of a mechanism that protects the network's integrity is necessary. The implementation of security in this network is challenging mainly due to limitations in the lifetime of a network and energy, which is consumed at high rates in the transmission of data across the network. [6]To overcome this, a reduction in the transmission overhead needs to be performed.

Most of the work done for the management of aggregation of data in an energy efficient manner such that the network is protected from data breaches have usually ignored the process of authentication as it is difficult to achieve the same by maintaining energy efficiency. [8]Not much effort has been made to overcome shortcomings like a security key and a base stations node's key length. Hence integrity of data is compromised.

Secure and Energy-Efficient Data Aggregation (SEEDA) - an extension of SDAACA protocol addresses this issue by creating an arbitrary timestamp and value with a hidden key. The node at the base station validates the fake aggregated data when the packets are received using the priorly generated key.

The key generated earlier is used for verification of unauthorized (used in place of fake) aggregated data by the node representing the base station on the reception of packets.

Secure node authentication is employed to detect and prevent the attacks by employing data fragmentation algorithms, fully homomorphic encryption, and access control model.

Network delays are overcome as the node representing the base station uses the information for the distance between the participating nodes.

The reliability of the method proposed is verified by creating several scenarios in which called Sybil and sinkhole attacks are introduced and by performing simulations their effects are observed.

The outcome of the simulation depicts that this protocol outperforms SDA, SDAT, SDALFA, EESSDA, SDAACA, and EESDA protocols in terms of security and energy consumption.

B Protection of Software-Defined Networking (Sdn)

Software-Defined Networking (SDN) enables the data and control parameters to be handled separately and a software program is used for controlling the overall functioning of the network.[20]
The centralized nature of SDN makes the controller vulnerable to attacks of distributed denial-of-service (DDoS).[17]

The past recommendations to overcome this can be categorized into two divisions.[7]

Network traffic analysis and controller capacity scale-up: This method is used against DDoS by adopting a process of filtration and detection against the forged flow based on a defined protocol.

Increase the capacity of the controller to handle greater processing workload under a DDoS attack. The limitations of the above methods include attainment of false values in case of improper filtering mechanism and increase in network overhead due to the deployment of multiple controllers to combat attacks by DDoS.

These limitations can be addressed by securing the control plane and the employment of a Safe-Guard Scheme (SGS) which involves a combination of positive attributes of the above-suggested methods.

SGS comprises two modules: anomaly traffic detection and controller dynamic defense. Anomaly traffic detection utilizes a four-tuple feature vector to segregate legitimate flows from forged ones.

Controller dynamic defense combats the effects of the DDoS attack by remapping the controller and ending access control to the data plane.

The outcome of the simulation obtained by experimentally evaluating SGS using Ryu and Mininet controllers verifiesits efficacy.

C Access Model for Wireless Powered Communication Networks

Wireless powered communication networking (WPCN) is a networking model where the power backup of machines which are part of a wireless communication environment are recharged in isolation by the utilizing microwave Wireless Power Transfer (WPT) [13] technology hence eliminating manual involvement in the replenishment of the battery. Challenges include decreased efficiency over large distances, the convoluted design of joint wireless information and intra-network transfer of power [21].

This can be alleviated by the employment of a relay-enabled wireless-powered communication network (WPCN), consisting of a relay-hybrid access point (RHAP), nodes for harvesting and transmission, and a base station (BS). Once the RHAP sends a signal the nodes harvests energy required for the information to be transmitted by way of RHAP.

The paper suggests the employment of a new distributed medium access control (MAC) mechanism in a relay WPCN, based on carrier sense multiple access with collision avoidance, a binary exponential random back-off mechanism. The proposal implies that the nodes and the RHAP utilize different window sizes with respect to contention, for channel access. In addition to it, windows with smaller sizes are assigned to the RHAP which results in it having a higher preference for channel access. Markov chain model for the proposed-MAC and a Markov chain model for the energy states of the nodes is proposed. This is used to mould the conduct of changing states between data transmission and energy harvesting.

The simulations exhibit the efficacy of the suggested concept in terms of energy and throughput.

D Applications

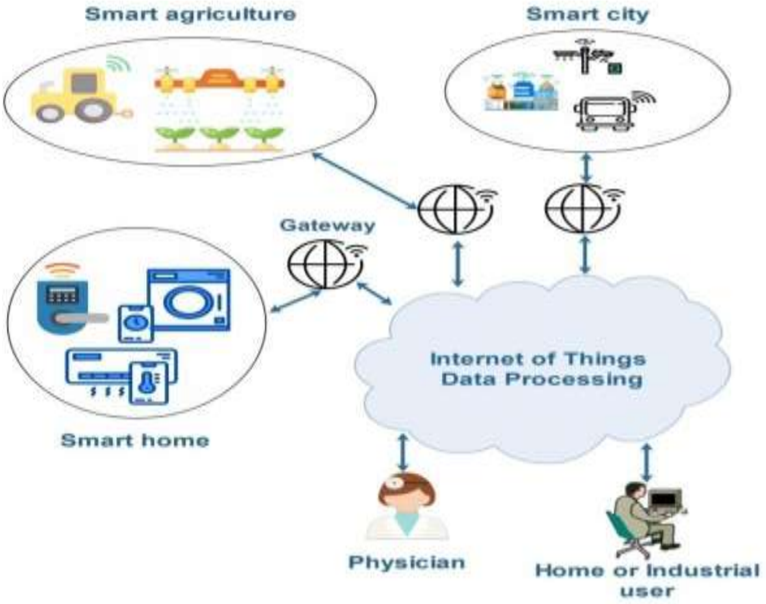

Figure 1. Applications of IoT

IoT is a prime example of networks where access control plays a huge role. With the multi-fold increase of devices connected today, the need for security also increases exponentially. Figure 1 describes a general IoT system with devices connected to it.

E Secure Device Access Control Mechanism for IoT

In IoT systems, having reliable d2d communication is important. Thus, an access control mechanism can help authenticate the devices without an intermediate system. With a secure key exchange mechanism in place, the communication system is fortified.[12]

Prior research introduced a lightweight access control and key agreement scheme (LACKA-IoT) and claimed that it was invulnerable to man-in-the-middle attack and device impersonation. This proposal refuted this claim by first proving that it is vulnerable to both and then proposed an improved protocol called iLACKA-IoT. The new scheme addresses formal and informal validation by proffering adequate security standards. This scheme's efficiency is also better than that of its predecessor. iLACKAIoT achieves access control and establishes the keys in 22.4512 ms and by exchanging 2944 bits. The proposed scheme has decreased the computation by 39.7% and the communication overhead by 12% as compared to its previous scheme. It is therefore a viable scheme for deployment in real-life scenarios.

F Dynamic Risk-Based Access Control System forIot

IoT has revolutionized the world by creating smart alternatives for everything. As reported by Cisco, there will be about 50 billion IoT devices by 2020.[11] All of these devices will be communicating with each other in real-time and will need real-time responses.

IoT devices principally are functional and must give maximum output by utilizing the least possible resources at the best price point. Thus, the security aspect of the communication of these devices still is underdeveloped. This paper proposes a system which will use external factors and real-time data such as user context, resource action severity, sensitivity, and risk history to give dynamic feedback. The model uses features that are adaptive to detect any discrepancies from the usual behavioral patterns of the verified users.

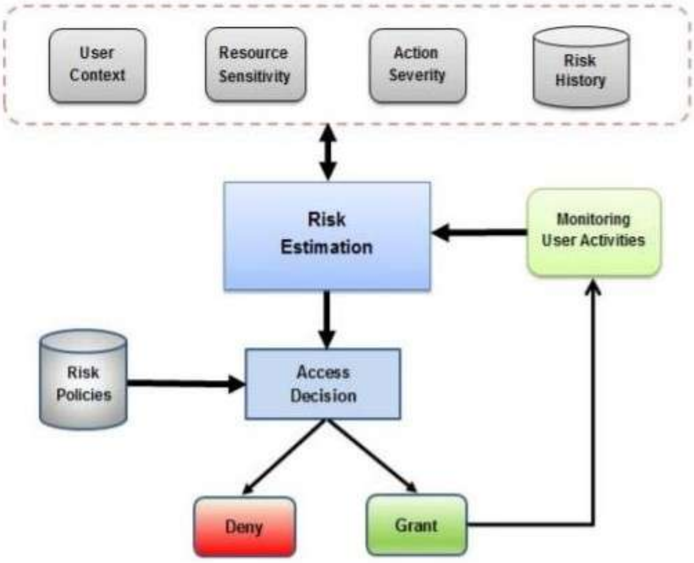

Figure 2. Flow chart of a Risk Based Access Control System

Figure 2 displays a risk-based access control system. It takes inputs from the environment. The system simultaneously monitors the authorized users for suspicious activity or change in behavioral patterns. When these two parameters are jointly considered, the protocol comes upon an access decision to grant or deny access to a particular user based on the risk policies.

G Access control mechanism for efficient M2M communication

Machine-to-machine (M2M) interactions allow free communication between devices which eliminates human efforts to form a novel facility, example - IoT and a smart grid.[8] The M2M environment consists of multiple machines that support a range of facilities required for communication of the sensors. As a result of which simultaneous and tremendous access breaches by MTCDs to radio access networks (RANs) results in the inefficient transmission of information. The paper's approach is to overcome degradation in performance due to simultaneous enormous attempts to access the LTE system by the MTCDs using Physical Random-Access Channel (PRACH) access control and resource allocation mechanism. This includes the development of an optimization issue to enhance the efficiency of random access with delay limitation.

Depending on the results of the estimation, an access control mechanism operating dynamically and algorithm based on resource allocation using RACH is developed. An embedded Markov chain-based model for investigating the technique is employed. Simulations are used for validation of the model, the results of which demonstrate the algorithm's effectiveness.

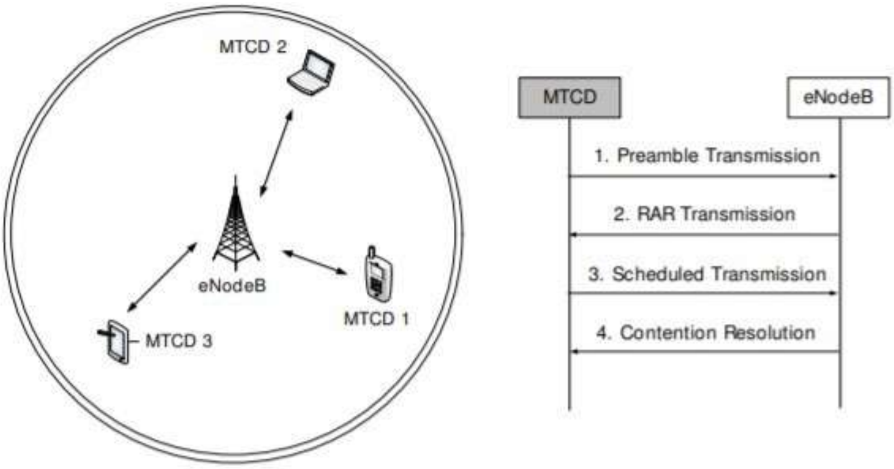

Figure 3. Signaling steps for random access in an LTEA

Depiction of the steps in random access process in Figure 3. comprises of the following steps:

Transmission of Preamble: preamble is transmitted by a MTCD through PRACH subframe.

In the second step, Random Access Response (RAR) Transmission, the MTCD waits to receive the RAR that consists of data required for transmission of uplink. After successfully checking and decoding the preamble, the eNB transmits the RAR to the MTCD. Collision of preambles occur if MTCDS send equivalent preambles in equivalent PRACH subframe, and hence detection is not achieved. In such cases, process of transmission is repeated. On successful reception from the eNB, Scheduled Transmission takes place. LTEA can be successfully accessed by MTCD on fruitful reception and decryption of contention resolution message.

H Access control mechanism for 5G and IoT

5G and its enhancements aim to achieve exceptional connectivity. Even though the prime focus is broadband communication, the approach is to achieve enhancements with respect to time-sensitivity and location-based resources amongst other applications [9]. IoT is essentially the environment of a connected device in which devices communicate over the internet for direct device to device communication with least human interference.

The continuous development of both has accompanied an increase in heterogeneity in structure, diversity of users, advanced services, and huge data. The enhancements have increased the requirement of an efficient secure mechanism to inhibit unauthorized access.[10]

Available security measure fails to eliminate hidden risks because of decreased isolation and unitary protection.

Multi-dimensional Fine-grained Control (MFC) framework aims to reinforce dependability and security for these systems. Isolation of the network is achieved by employing an identifier mapping mechanism. Comparison of various policies is performed to analyze MFC's. Furthermore, an integrated authentication prototype paradigm is designed with external parameter settings for the wireless system. Scenarios for verification are implemented for testing the effectiveness of the framework. Results obtained depict the framework is viable for applications utilized in IoT or 5G.

IV Conclusion

This paper successfully covered Network Access Control, the types of access control and various protocols in the same. We also covered network security and the schemes to ensure privacy, accountability, authorized access, prevent data leakage and tampering along with ciphertext authentication. We then reviewed protocols and methodologies to improve some pre-existing schemes in terms of security and their efficiency. Lastly, we viewed the applications of access control in IoT systems.

References

1. J. Wei, G. Yang and Y. Mu, "Comments on "Accountable and Privacy- Enhanced Access Control in Wireless Sensor Networks"," in IEEE Transactions on Wireless Communications, vol. 15, no. 4, pp. 3097-3099, April 2016
2. J. Shi, R. Li and W. Hou, "A Mechanism to Resolve the Unauthorized Access Vulnerability Caused by Permission Delegation in Blockchain-Based Access Control," in IEEE Access, vol. 8
3. S. Ding, J. Cao, C. Li, K. Fan and H. Li, "A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT," in IEEE Access, vol. 7.
4. F. Li and J. Hong, "Efficient Certificateless Access Control for Wireless Body Area Networks," in IEEE Sensors Journal, vol. 16, no. 13
5. M. Uddin, S. Islam and A. Al-Nemrat, "A Dynamic Access Control Model Using Authorising Workflow and Task-Role-Based Access Control," in IEEE Access, vol. 7
6. A. A. Jasim et al., "Secure and Energy-Efficient Data Aggregation Method Based on an Access Control Model," in IEEE Access, vol. 7, pp. 164327-164343, 2019 [7]Y. Wang, T. Hu, G. Tang, J. Xie and J. Lu, "SGS: Safe-Guard Scheme for Protecting Control Plane Against DDoS Attacks in Software-Defined Networking," in IEEE Access, vol. 7, pp. 34699-34710, 2019
7. C. Oh, D. Hwang and T. Lee, "Joint Access Control and Resource Allocation for Concurrent and Massive Access of M2M Devices," in IEEE Transactions on Wireless Communications, vol. 14, no. 8, pp. 4182-4192, Aug. 2015

8. A. Ghosh, A. Maeder, M. Baker and D. Chandramouli, "5G Evolution: A View on 5G Cellular Technology Beyond 3GPP Release 15," in IEEE Access, vol. 7, pp. 127639- 127651, 2019
9. Z. Ai, Y. Liu, L. Chang, F. Lin and F. Song, "A Smart Collaborative Authentication Framework for Multi-Dimensional Fine-Grained Control," in IEEE Access, vol. 8, pp. 8101-8113, 2020
10. H. F. Atlam, A. Alenezi, R. J. Walters, G. B. Wills and J. Daniel, "Developing an Adaptive Risk-Based Access Control Model for the Internet of Things," 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, 2017
11. S. A. Chaudhry, K. Yahya, F. Al-Turjman and M. -H. Yang, "A Secure and Reliable Device Access Control Scheme for IoT Based Sensor Cloud Systems," in IEEEAccess, vol. 8, pp. 139244-139254, 2020
12. A. Iqbal, Y. Kim and T. Lee, "Access Mechanism in Wireless Powered Communication Networks With Harvesting Access Point," in IEEE Access, vol. 6, pp. 37556-37567, 2018
13. C. Blundo, S. Cimato and L. Siniscalchi, "Managing Constraints in Role Based Access Control," in IEEE Access, vol. 8, pp. 140497-140511, 2020
14. S. Li, W. Ren, T. Zhu and K. R. Choo, "Lico: A Lightweight Access Control Model for Inter-Networking Linkages," in IEEE Access, vol. 6, pp. 51748-51755, 2018 [16]Lakbabi, Abdelmajid. (2012). Network Access Control Technology— Proposition to Contain New Security Challenges. Int'l J. of Communications, Network and System Sciences.
15. W. Fan and F. Yang, "Centralized Trust-Based In-Band Control for SDN Control Channel,"in IEEE Access, vol. 8, pp. 4289-4300, 2020, doi: 10.1109/ACCESS.2019.2963475.
16. F. Yan, Y. Jian-Wen and C. Lin, "Computer Network Security and Technology Research," 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation, Nanchang, 2015
17. A Review paper on Network Security and Cryptography Dr. Sandeep Tayal1 , Dr. Nipin Gupta2 , Dr. Pankaj Gupta3 , Deepak Goyal4 , Monika Goyal5 1,2 Associate Professor ECE, Vaish College of Engineering, Rohtak (H.R), Inida. 3Professor, CSE, Vaish College of Engineering, Rohtak (H.R), Inida. 4Associate Professor, CSE, Vaish