

MODELING OF A COLLECTIVE APPROACH FOR SECURING COMMUNICATION OVER CONTENT- CENTRIC NETWORKS IN THE PERSPECTIVE OF FIA

Vidya M.S

Assistant Professor,
Department of Computer Science & Engineering, BMSIT& M, Bangalore, India,
Email: rvidyapai@bmsit.in

Mala C Patil

Assistant Professor,
Department of Computer Science,
COHB University of Horticultural Sciences, Bagalkot, India,
Email: malapatil2002@yahoo.co.in

Dr. Shiva Murthy G

Associate Professor,
Department of CSE, VTU PG Centre Muddenahalli,
Bangalore India
Email: kgshivam@gmail.com

Abstract

Software defined networking (SDN) plays a very important role to define enhanced content centric network for Industry 4.0 future internet architecture. The primary objective of the future internet architecture foundation is to provide better content delivery among various forms of connected objects. It also aims to connect enormous amount of physical objects through heterogeneous operating communication protocols. The communication protocols are mostly being designed taking three crucial factors into account- i) Scalability, ii) Interoperability and iii) Security for network and physical layer attributes. However, the conventional form of host IP centric protocols such as IPV4 and IPV6 generate communication burden when considered in the context of FIA and also do not ensure significant security measures for FIA. Thereby, it is necessary to redefine a solution taking the baseline reference architecture of novel security policies which can balance the communication performance and security trade-off by identifying potential security threats. This research study introduces a combine framework of data security aiming the futuristic Internet hosting services for content centric networks. The system is analytically conceptualized with two different novel algorithms which are tested under variable operating conditions and different set of data. The outcome exhibited that both the security mechanisms poses computational efficiency by boosting secure communication at SDN in FIA.

Keywords: Future Internet Architecture; Software Defined Networking; Security; Computational Efficiency.

1. Introduction

The foundation of existing traditional architecture of Internet based communication is being operational since last three to four decades. Till date the baseline architectural components of internet services have been successfully evolved to launch and align various technological features in order to fulfill the demand and requirements of modern ubiquitous applications. However, the successful implementation of various distributed content specific components also extended the potential features of routing designs and also attempts to ease the communication for all possible user needs [1]. As the requirements to operate various ubiquitous streamline

applications slowly taking a paradigm shift towards futuristic Internet Architecture (FIA) which targets to implement Internet-of-Things (IoT) as a services with infrastructural backbone of complex mode of 5G and its legacy versions. Hence, the conventional internet architecture lacks efficiency to cope up with the advanced mode of communication with increasing demands of content-centric decentralized applications [2] [3]. The current evolution in the research trend of cross domain of software defined networking (SDN) and content delivery services clearly exhibits the fact that the initiation of transformation from traditional internet based applications are taking paradigm shift towards the FIA but the traditional security approaches not more potential when taken into account for FIA secure communication systems due to various factors. Such as- i) Firstly, the current era of distributed computing requires highly interoperable security mechanism due to heterogeneity of integration of networking technologies where the conventional host-centric IP network do not offer better security at TCP/IP link layer communications for medium access control (MAC) layers. ii) Secondly, multi-cast IP routing with different routing policies encountering several IP-conflicts and exhaustion issues as the number connected static and mobile users to voice over internet protocols (VoIP) and other IP-enabled communication systems are increasing with limited infrastructure of communication., iii) Thirdly most of IP based communication do not involve much security attributes, although in the case of IPV6 unique allocation of IP promote security to an extent. iv) Majority of the conventional techniques do not offer better performance in terms of scalability and robustness and that confine it to be evolved with modern communication access technologies [4]. This also makes it impediment towards successful implementation in the context of FIA [6]-[12]. The prime aim of the proposed research study is to come up with a novel security solution where inclusion of two major computational approaches targets to improve the data security and access control policy in the context of FIA systems. The numerical modeling of the framework combines two different approaches where 1st-functional core module enables high-level security to make the communication of content centric network more defensive against different form of intrusion. Whereas on the other hand SDN based switching is incorporated to make the communication of FIA more secure. The pattern followed to make this manuscript more organized is as follows: Section 2 introduces the relevant studies focused on security of FIA, whereas section 3 derives and outlines the research problem. Section 4 and Section 5 discusses about the research methodical design and algorithm implementation details respectively followed by result and discussion in Section 6. Finally Section 7 concludes the overall research outcome.

2. Related Work

The conventional architectural backbone corresponding to internet services poses a discrete condition of real-time network bottlenecks on data flow. This condition usually refers to a situation where data flow among the communication resources become limited and restrict the system to be scaled up with collaborative IoT applications requirements to solve specific user demand. The study of (T. Huang, F. Richard Yu, G. Xie, and Y. Liu, 2017), also emphasized on analyzing the requirements of FIA and claimed that apart from the scalability issue the conventional way of Internet based communication and networking technologies also do not perform efficiently when synchronous mode of communication is highly desired with mobility factors. The conventional communication mechanisms are also not much suitable for advanced on demand content distribution for different IoT applications. The crucial factors which make it difficult are i) non-flexibility among the network components along with ii) Inclusion of computationally constrained control mechanisms [13]. To handle the scalability, issue an extensive work have been carried out with the evolved structure of 32-bit of addressing mode of IPV4 to 128-bit IPV6. (W. Ding, Z. Yan and R. H. Deng, 2016) reviewed different versions of IP based Internet communication protocols and claimed that 128-bit addressing mode of IPV6 can address the scalability problem to some extent in the context of FIA. The study also claimed that although it can handle the scalability problem but lacks efficiency when host-centric IP enabled network is operationally combined with the context of distributed communication systems and advanced paradigm of collaborative architecture oriented applications [14]. This basically require open architecture of internet based applications. There are very less studies explored the potential of IPV4 and IPV6 towards strengthening the security aspects of FIA , however few significant related studies such as (S. Kent and K. Seo, 2005) [15] , (R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, 2005) [16] , who has adopted the techniques of IPSec and DNSSec to improvise the security aspects of IPV4 and IPV6 where it has also derived its wider scope of applicability into the FIA communication systems which collaborates 4G , 4G-LTE and 5G infrastructural backbone to support high-speed and high dimensional content delivery for various IoT application based services. A security plan for protecting the control plane against Distributed DoS attacks is presented in the study of Wang et al. [17]. The important quality of this approach is the deployment of multiple controllers in the control plane through a cluster of controllers. Yang et al. [18] suggested a method designed based on the joint approach of anomaly identification and a multi-layer response model. Anomaly identification checks for abnormal behavior from the state of the physical process and a multi-layer response model prevent unauthorized packet communication, thereby generating a strategy to mitigate attacks to protect the physical process. Geng et al. [19] have suggested dual security strategies for vehicle

network. Initially, the network hierarchy was composed of software-defined concept to normalize the network management. Based on this fact, various security protocols are embedded to prevent common security attacks in the network. Meng et al. [20] concentrated on detecting insider attacks in clinical SDN. Here, the author first conducted an investigation and designed a trust-based method using Bayesian inference to find malicious devices in a medical environment. Wang et al. [21] presented a security mechanism to resist DoS attacks in the SDN controller. The presented security mechanism mainly includes multiple implementation modules such as DoS detection module, forecasting engine module, priority manager module, and the last one is the scheduler module. The performance of the presented approach is assessed in terms of OpenFlow environments. The study outcome demonstrates that the presented approach is efficient for ensuring robust security with limited overhead. Achleitner et al. [22] defined a strategic method to prevent network services against network reconnaissance and designed a reconnaissance deception system. The main purpose of this method is to cancel information of the attacker, and delayed the operation of finding vulnerable hosts, and determined the source point of attacks in the network. In the study of Xu et al. [23], a review work is performed to examine the impact of the table-overflow attack on the SDN. The authors found that the existing solutions are not much suitable to defend such kinds of attacks in the SDN-oriented network system. In order to overcome the limitation of existing solutions, the study has presented an attack detection mechanism based on traffic features and mitigation mechanisms using a token bucket scheme. Yan et al. [24] suggested a scheduling approach using a time-slice allocation mechanism to ensure the availability of SDN services under a distributed-DoS attack. Similarly, the work of Yoon et al. [25], have also carried a comprehensive study towards attacks in SDN OpenFlow network. Here, the author discusses the taxonomy to gain understanding into general pitfalls that make SDN stacks corrupted under hostile computing environments. The work of Deng et al. [26] revealed a different form of vulnerability associated with SDN and introduced a packet injection attack than creating a bad impact on the network topology management and rest API, on the SDN controller. The authors then designed a lightweight mechanism of the packet-catcher existing SDN controller to mitigate the impact of this attack. Lal et al. [27] suggested a hybrid scheme that includes physical layer security, SDN, node collaboration, context awareness, and cross-layer. The suggested scheme implements at both nodes level and network-level those are compatible with network conditions, and possible attacks.

3. Research Problem

In order to understand the need of research, it is essential to see the benefits of Future Internet Architecture (FIA) and to highlights the problems that acts as impediment towards successful implementation.

3.1 Problem Context-1: Research Problems addressed in the context of Data Security Mechanism

There are various literatures to claim that CCN is an integral part of FIA, but there is no discussion of an implementation to boost up the data security. Existing researchers working on cloud security has dominantly used public key encryption without assessing their computational complexity as well as response time. It is quite evident that public key encryption will consume more resources as well as computational processing time if they are allowed to work on highly distributed environment irrespective of their claimed reliable security. At the same time, existing key management techniques over cloud computing as hosting existing internet architecture doesn't offer full fledged secret key security. It cannot ensure both forward and backward security at same time during algorithm implementation. In this entire scenario of implementation, it can be seen that data, which is primarily content in CCN is never safe when allowed to be transmitted in highly distributed channels in FIA. Dependencies over third party application do exists today but in such cases the ownership of the data as well as privacy information of the data (or content) owner is at greater risk. Therefore, there is a need to design a fail-proof access control system that is capable of identifying the legitimate user over cloud and permit them access without involving much complicated steps of authentication. At the same time, the user's private data as well as owned content are required to be kept on top priority while performing secure communication over applications running on FIA.

3.2 Problem Context-2: Research Problems addressed in the context of Access Control Mechanism

There are various literatures to claim that SDN is one of the integral parts of FIA as it is capable of performing classification of higher order granularity to facilitate superior routing behavior in FIA. However, none of the research approaches on security-based solutions on FIA has ever explored or addressed the security pitfalls associated with SDN based FIA system. Basically in SDN, the connectivity among different planes (application, control, and data) is highly limited and this limited feature could be misused by the intruder that could inflict damage on the switching system of SDN. Although, there are solutions for different forms of attack in FIA reported in literatures, but all these reported attacks have something in common i.e. these attack strategy uses nearly similar strategy to launch its attack. The strategy is to send random and distinct packets to the switches and consistently engages the switching process thereby paralyzing the controller in FIA. These results in

permanent communication failure between the communicating devices and servers in any form of FIA constructed using SDN. At the same time, consideration of SDN is inevitable in FIA system owing to its routing capabilities over distributed system. It was also found that solutions of existing research approaches usually perform excessive communication between the controller and switches that leads to abnormal increase in bandwidth consumption in SDN. This phenomenon leads to an entry of all sorts of attack with lesser chances to even identifying them. Therefore, there is a need of highly secure scheme that could perform more effective access control system that could offer more enhanced level of communication and data security.

Thereby the problem statement of the study can be derived as- **“To ensure that proposed SDN based routing and switching operation in FIA offers faster response time for identifying and mitigating all sorts of major threats”**. The proposed system is an extension of our prior model [28] [29].

4. Research Methodology

The prime purpose of the proposed system is to design and develop a secure mechanism to safeguard the communication process in future internet architecture. For this purpose, the implementation of the proposed system is carried out in order to accomplish two research objectives as the contribution viz. i) To develop a novel framework of data security for facilitating resilient communication over content centric network in FIA, and ii) To design a novel access control system that can perform identification of major threats followed by isolation of it in SDN based switching system in FIA. The architecture of the proposed system is as follows:

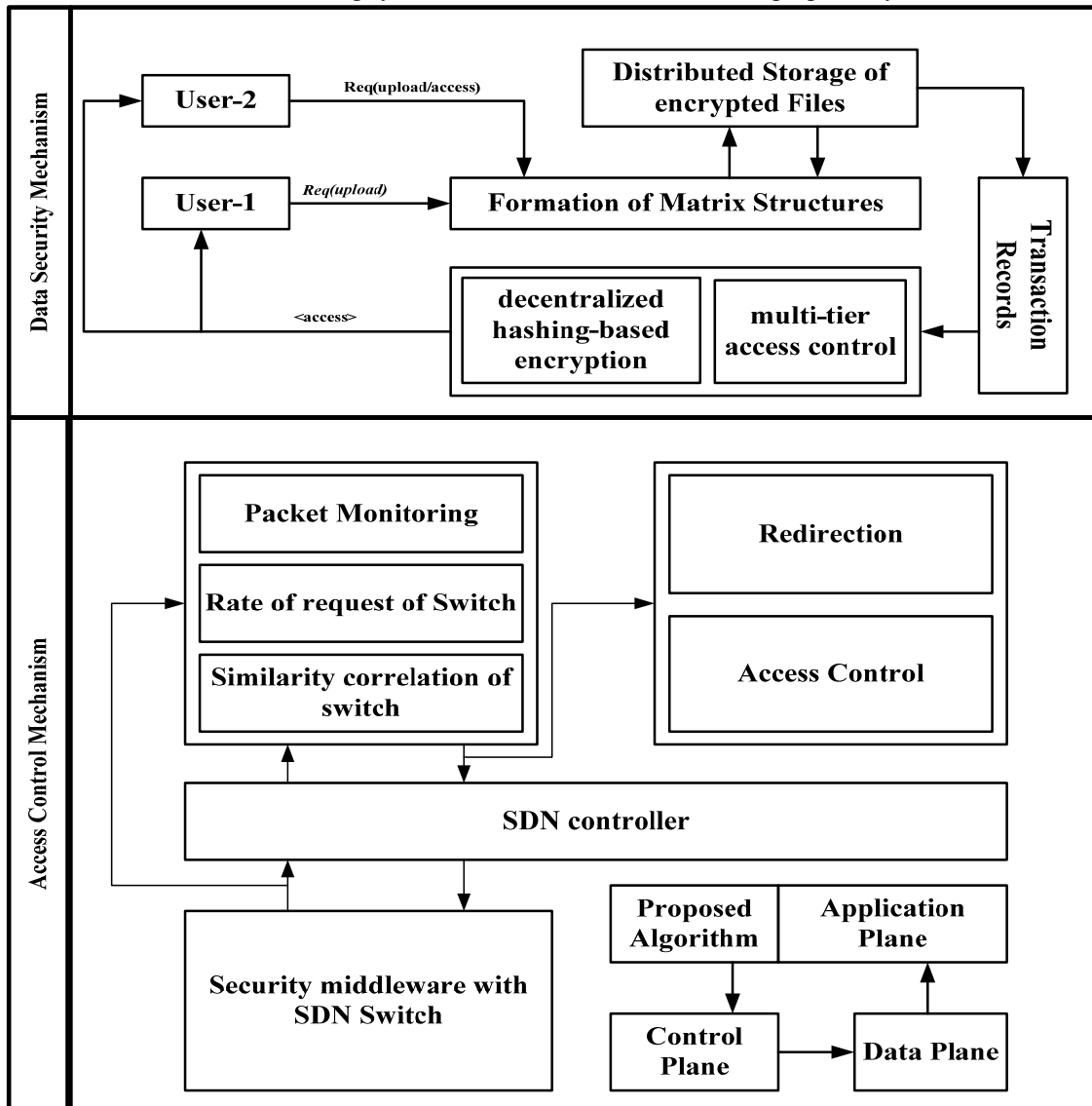


Fig.1 Architecture of Proposed System

Fig.1 highlights that the solution towards strengthening the security system in future internet architecture consists of two phases of operation viz. i) data security phase and ii) access control phase. The first phase of

implementation is focused on using a decentralized hashing-based encryption mainly emphasizing on achieving data security in presence of lethal attacks like cross-scripting over various web-contents hosted in cloud. The second part of the implementation further focuses on access control considering three significant planes of software defined network viz. application plane, data plane, and control plane. The system introduces *multi-tier access control* policy that lets the user upload ciphered data along with an arbitrary security token. The proposed system deploy a matrix-structure that will reposit all the legal transaction that are subjected to hashing as well as encoding in order to formulate a secure tree like structure. One of the essential contributions of the proposed implementation planning is not to use any form of cryptographic policy for designing access control policy. An algorithm will be constructed to check if the data packet has any form of correlation with existing or prior traffic flows in its cache.

5. Algorithm implementation

This section discusses about the algorithms that has been implemented for proposed system:

5.1 Robust Data Security over Content Centric Network

This paper dimension includes a new scheme of the context security for FIA for securely sharing the content by handling the trade-off of the degree of security level and resource overheads. The method adopts a decentralized hashing operation to secure the content by developing a multi-tier block-based access control policy where the user uploads a ciphered data along with an arbitrary security token. A tree-structure represents the data and the transactional details, where the algorithm does not consider any personal information into any of the transaction to provide the user's privacy. The deciphering process adopts a pointer based addressing scheme without having any dependencies on the user's profile data. The efficient matrix-based structure keeps records of all the legal transaction of hashed and encoded structure to form a secure tree like structure. The scheme extracts the security blocks from the secure tree structure and recursively generates a new set of matrix structure with a link of edge among them. Therefore, the content integrity over a distributed and decentralized FIA is achieved, where it is very hard to alter the data and the auditing process of the content integrity is achieved with optimal overheads to facilitate content security and integrity with authentication together is achieved only by hashing based operations.

Algorithm for content-centric encryption

Input: n (data)

Output: u_{data} (decrypted data received by user)

Start

1. **For** $i=1:n$
2. $Cdata = f(n)$
3. **For** $j=1:m$
4. *construct* block $gen_token(Cdata)$
5. **End**
6. distribute block u
7. $u_{data} = tag(block)$
8. **End**

End

The algorithm takes the input of n (data) that after processing yields and outcome of u_{data} (decrypted data received by user). For all the data obtained in the forwarding process, the ciphered data is obtained by using hashing function $f(x)$ (Line-2). The next part of the study is about constructing block for the maximum value of hash m (Line-3). The blocks are constructed by applying a function gen_token that takes the input of ciphered data $cdata$ (Line-4). After the blocks are obtained, the hash values of the blocks are now ready to be assigned to each user u (Line-6). The final stage of implementation is about applying a discrete encryption operation towards the finally obtained hash value of the blocks for facilitating the extraction of user data u_{data} (Line-7). This will complete the decryption process. Therefore, it can be seen that irrespective of any inclusion of any complex cryptography, the block-based access policy offers potential security towards the data forwarding process among the IoT devices in distributed networks

5.2 Access Policy for Boosting Secure Communication

The prime aim of the proposed study is to develop a mechanism of a distinct access control in order to identify lethal threats associated with cross scripting attack over future internet architecture. The algorithm for this purpose is as below:

Algorithm for Secure Route Construction

Input: P_{sw} , E_{sw} , S

Output: r

Start

```

1. init  $P_{sw}, E_{sw}, S, c_{capd}, c_{cap}$ 
2.  $d_{entry} = [ProfID, CSLoC, UT, CS]$ 
3. generate jobs( $P_{sw}, E_{sw}, S, u$ )
4. For  $i=1: S$ 
5.   For  $j=1: c_{cap}$ 
6.     For  $k=1: size(d_{entry})$ 
7.       obtain zone of current request
8.       compare each zone
9.     For  $l=1:S_{rem}$ 
10.       $N=N(l)+1;$ 
11.    End
12.     $N=N(rix)$ 
13.    Compute  $Ms \rightarrow V_{cap} / V_{slice}$ 
14.  End
15. End
16. End
17. apply  $f(x)=r$ 
End

```

The algorithm takes the necessary input for modeling user request that consists of profile identity $ProfID$, content server location $CSLoC$, upload time UT , content size CS (Line-2). All this information is retained in a matrix d_{entry} (Line-2) while other related software defined network variables of switching are also initialized e.g. prime switch P_{sw} , edge switch E_{sw} , number of server's S (Line-1). The algorithm considers demand of channel capacity c_{capd} , which is initiated, along with other variables. The jobs are generated on the basis of matrix d_{entry} and random allocation of c_{capd} . The consecutive evaluation is carried out considering all the servers S (Line-4), channel capacity c_{cap} (Line-5), and all the rows of the matrix d_{entry} (Line-6). All the communication regions are compared logically with the elements of the d_{entry} matrix (Line-7 and Line-8). The next part of the algorithm implementation is about considering all the remaining servers S_{rem} (Line-9) and look for quantity of the server in each communication area. This computation (Line-10) is carried out considering the reduced number of virtual machine at each communication area. All the servers located at each communication area are then randomized where the variable rix represent a matrix holding all the random servers over each communication region (Line-12). The algorithm initializes capacity (V_{cap}) as well as slices of virtual machine (V_{slice}) in order to obtain the memory occupied per slice (Ms) as shown in Line-13. The function $f(x)$ performs two significant tracking attributes viz. the rate of request from switch as well as the similarity correlation of the switches. This operation is constructed in order to distinguish malicious traffic and regular traffic.

6. Result and Discussion

This section exhibits the visualization of the outcome and also discusses the numerical analysis corresponding to algorithm time complexity. The entire methodology is realized with respect to extensive analysis considering numerical computing platform where both communication and security factors are concerned for two different frameworks such as i) Framework for data security mechanism and ii) Framework for access control.

6.1 Analysis of framework for data security mechanism

The outcome clearly shows that the formulated concept of data security scheme outperforms the conventional SHA-1 and SHA-2 shown in fig.2.

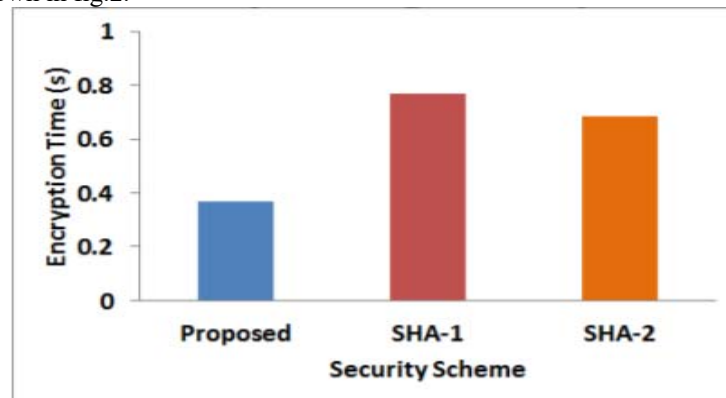


Fig.2 Analysis of encryption time

The quantified outcome shows that the formulated system attain encryption time of ~0.4 sec which is quite lesser as compared to SHA-1 and SHA-2. In the case of SHA-1 the estimated encryption time obtained is ~0.8

sec and in the case of SHA-2 it is found ~0.73 sec. Thereby from the performance view point the formulated encryption poses faster mode of execution flow as compared to SHA-1 and SHA-2.

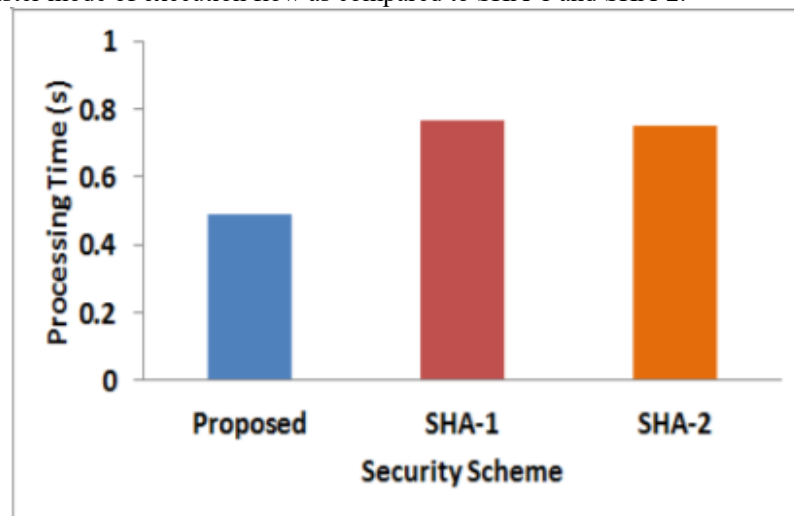


Fig.3 Analysis of processing time

The complexity analysis on the basis of algorithm processing time also shows that the proposed algorithm attain very negligible time complexity as compared to the existing SHA-1 and SHA-2 is shown in fig. 3.

6.2 Analysis of framework for Access Control mechanism

This segment of the result analysis shows (fig.4) the comparative outcome obtained after simulating the framework for access control mechanism and also justify it with respect to different performance measures.

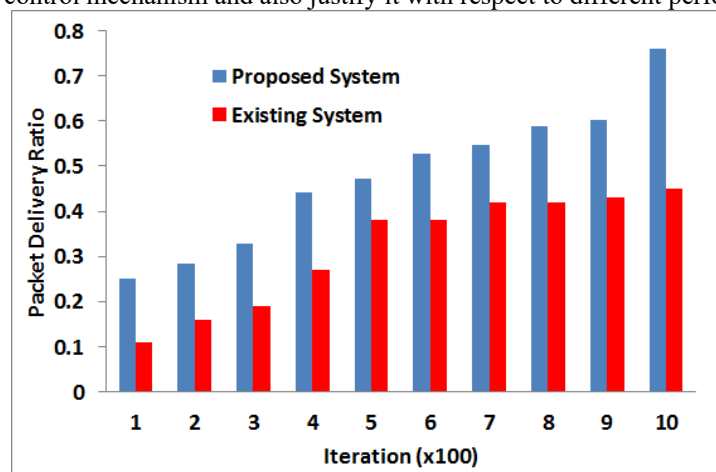


Fig.4 Comparative Analysis of Packet Delivery Ratio

The proposed system is compared with the existing encryption approach used for resisting cross-scripting attack in future internet architecture (Shown in fig.5). Various encryption approaches e.g. SHA-1, SHA-2, AES are applied and outcomes are averaged in order to compare with the proposed system with respect to packet delivery ratio and % of attack mitigation.

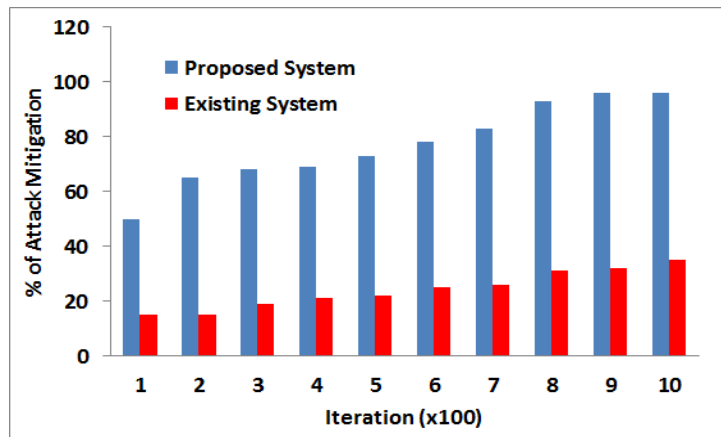


Fig.5 Percentage of Attack Mitigation

The percentage of attack mitigation is evaluated by computing number of confirmed identified attack and number of suspicious traffic that has been isolated. The outcome in Figure 5 shows that proposed system has significantly better identification rate compared to existing algorithms of security. The prime reason behind this performance is that proposed system makes use of packet monitoring approach using cost effective routing strategy. Hence, more information is relayed by the nodes in software defined network where the controller can undertake appropriate decision for resisting the malicious routes infected by the cross scripting attack. Unfortunately, existing encryption approach is iterative and not-flexible which fails them to identify the attack routes.

6.3 Time complexity

As per the proposed logic, when a routing takes place with an aid of a controller system over software defined network, it performs flagging of all the nodes that are involved in the route. This is hypothetically in order to exhibit that there is a confirmed path. However, in the continuation of the process of secure route exploration in future internet architecture, if the search converges to one of the indexed node than it reports back about the presence of single hop path. The search process is termed successful and secured routes are updated. Hence, the computation of the time complexity can be carried out as follows:

$$T_{comp}(N, A) \rightarrow O(B_1) + A.B_2 \dots \text{(eq.1)}$$

In the above expression of time complexity T_{comp} , we used big O notation where the variable N and A represents total number of user and adversaries. The variable B_1 represents duration that is needed to search and identify the vulnerable node (using our algorithm) over cloud while B_2 represents duration required for searching the attacker node. In the most extreme situation, the logical condition generated by the A number of attacker node is assumed than it will lead to $B_1=O(A)$. Similarly, search for the attacker node is actually about finding the similarity correlation as well as it also includes all the cloud users which is vulnerable or susceptible to be compromised. A threshold of idea significance value of 0.05 can be used to confirm this fact from the correlation analysis. Here also, in extreme scenario, there is a possibility of presence of attacker or compromised node in all the host. Such scenario will result in $T(B_2)=O(N)$. Therefore, the total complexity of time can be updated as,

$$T(N, A) = O(N * O(A) + e * O(N)) \dots \text{(eq.2)}$$

The above expression actually means $T(N, A)=O(N,A)$. hence, until all the adversaries are quite high in number in comparison to given network size, the proposed system results in polynomial of time. This is not much possible in real-scenario case. Table 1 to Table 3 highlights the time complexity scenario considering three difference cases.

Table 1 When A is Constant Throughout

N	A	N*A
10	5	50
50	5	250
100	5	500
150	5	750
200	5	1000
250	5	1250
300	5	1500

Table 2 When N is Constant Throughout

N	A	N*A
10	5	50
10	10	100
10	15	150
10	20	200
10	25	250
10	30	300
10	35	350

Table 3 Both N and A is constant throughout

N	A	N*A
10	5	50
10	5	50
10	5	50
10	5	50
10	5	50
10	5	50
10	5	50
10	5	50

7. Conclusion




The research study introduces a combined security framework for SDN driven FIA to combat maximum possible threats in control and data-plane. For this purpose, it basically conceptualizes two different algorithms i) Algorithm for content centric encryption policy and ii) Algorithm for secure route construction in FIA. The concept is proposed to defend cross scripting attacks under variable traffic conditions. The experimental outcome shows that both the algorithms are tested under different dataset with variable workloads and poses the complexity $O(A)$ and $O(N)$ respectively. The time complexity analysis shows that the proposed approach is suitable to define better secure routing in FIA with well balance communication performance. It also exhibits that the system performance got improved to a significant extent which $\sim 82\%$.

References

- [1] B. van Schewick, Internet Architecture and Innovation, MIT Press, 2012
- [2] Ke Xu, Min Zhu, Guang Wu, "Towards evolvable Internet architecture-design constraints and models analysis", Springer-Science China Information Sciences, vol.57, Iss.11, pp.1-24, 2014
- [3] B. Zhou, Q. Shi and P. Yang, "A Survey on Quantitative Evaluation of Web Service Security," 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, 2016, pp. 715-721.
- [4] H. C. Huang, Z. K. Zhang, H. W. Cheng and S. W. Shieh, "Web Application Security: Threats, Countermeasures, and Pitfalls," in Computer, vol. 50, no. 6, pp. 81-85, 2017.
- [5] W. J. Buchanan, S. Helme and A. Woodward, "Analysis of the adoption of security headers in HTTP," in IET Information Security, vol. 12, no. 2, pp. 118-126, 3 2018.
- [6] M. Ambrosin, A. Compagno, M. Conti, C. Ghali and G. Tsudik, "Security and Privacy Analysis of National Science Foundation Future Internet Architectures," in IEEE Communications Surveys & Tutorials. doi: 10.1109/COMST.2018.2798280
- [7] Z. Su, Y. Hui and Q. Yang, "The Next Generation Vehicular Networks: A Content-Centric Framework," in IEEE Wireless Communications, vol. 24, no. 1, pp. 60-66, February 2017.
- [8] W. Ding, Z. Yan and R. H. Deng, "A Survey on Future Internet Security Architectures," in IEEE Access, vol. 4, pp. 4374-4393, 2016.
- [9] L. Kotut and L. A. Wahsheh, "Survey of Cyber Security Challenges and Solutions in Smart Grids," 2016 Cybersecurity Symposium (CYBERSEC), Coeur d'Alene, ID, 2016, pp. 32-37.
- [10] B. Stritter *et al.*, "Cleaning up Web 2.0's Security Mess-at Least Partly," in IEEE Security & Privacy, vol. 14, no. 2, pp. 48-57, Mar.-Apr. 2016.
- [11] R. Kozik, M. Choraś and W. Hołubowicz, "Packets tokenization methods for web layer cyber security," in Logic Journal of the IGPL, vol. 25, no. 1, pp. 103-113, Feb. 2017.
- [12] H. C. Huang, Z. K. Zhang, H. W. Cheng and S. W. Shieh, "Web Application Security: Threats, Countermeasures, and Pitfalls," in Computer, vol. 50, no. 6, pp. 81-85, 2017.
- [13] T. Huang, F. Richard Yu, G. Xie, and Y. Liu, "Future internet architecture and testbeds," in China Communications, vol. 14, no. 10, pp. iii-iv, Oct. 2017.
- [14] W. Ding, Z. Yan and R. H. Deng, "A Survey on Future Internet Security Architectures," in IEEE Access, vol. 4, pp. 4374-4393, 2016.
- [15] S. Kent and K. Seo, Security Architecture for the Internet Protocol, document RFC 4301, 2005.
- [16] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, DNS Security Introduction and Requirements, document RFC 4033, 2005.

- [17] 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.
- [18] J. Yang, C. Zhou, Y. Tian and S. Yang, "A Software-Defined Security Approach for Securing Field Zones in Industrial Control Systems," in IEEE Access, vol. 7, pp. 87002-87016, 2019.
- [19] R. Geng, X. Wang and J. Liu, "A Software Defined Networking-Oriented Security Scheme for Vehicle Networks," in IEEE Access, vol. 6, pp. 58195-58203, 2018.
- [20] W. Meng, K. R. Choo, S. Furnell, A. V. Vasilakos and C. W. Probst, "Towards Bayesian-Based Trust Management for Insider Attacks in Healthcare Software-Defined Networks," in IEEE Transactions on Network and Service Management, vol. 15, no. 2, pp. 761-773, June 2018.
- [21] T. Wang, Z. Guo, H. Chen and W. Liu, "BWManager: Mitigating Denial of Service Attacks in Software-Defined Networks Through Bandwidth Prediction," in IEEE Transactions on Network and Service Management, vol. 15, no. 4, pp. 1235-1248, Dec. 2018.
- [22] S. Achleitner, T. F. La Porta, P. McDaniel, S. Sugrim, S. V. Krishnamurthy and R. Chadha, "Deceiving Network Reconnaissance Using SDN-Based Virtual Topologies," in IEEE Transactions on Network and Service Management, vol. 14, no. 4, pp. 1098-1112, Dec. 2017.
- [23] T. Xu, D. Gao, P. Dong, C. H. Foh and H. Zhang, "Mitigating the Table-Overflow Attack in Software-Defined Networking," in IEEE Transactions on Network and Service Management, vol. 14, no. 4, pp. 1086-1097, Dec. 2017.
- [24] Q. Yan, Q. Gong and F. R. Yu, "Effective software-defined networking controller scheduling method to mitigate DDoS attacks," in Electronics Letters, vol. 53, no. 7, pp. 469-471, 30 3 2017.
- [25] C. Yoon et al., "Flow Wars: Systemizing the Attack Surface and Defenses in Software-Defined Networks," in IEEE/ACM Transactions on Network and Service Management, vol. 25, no. 6, pp. 3514-3530, Dec. 2017.
- [26] S. Deng, X. Gao, Z. Lu and X. Gao, "Packet Injection Attack and Its Defense in Software-Defined Networks," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 3, pp. 695-705, March 2018.
- [27] C. Lal, R. Petrocchia, K. Pelekanakis, M. Conti and J. Alves, "Toward the Development of Secure Underwater Acoustic Networks," in IEEE Journal of Oceanic Engineering, vol. 42, no. 4, pp. 1075-1087, Oct. 2017.
- [28] Vidya M.S., Patil M.C. (2019) A Novel Schema for Secure Data Communication over Content-Centric Network in Future Internet Architecture. In: Silhavy R., Silhavy P., Prokopova Z. (eds) Computational Statistics and Mathematical Modeling Methods in Intelligent Systems. CoMeSySo 2019. 2019 Advances in Intelligent Systems and Computing, vol 1047. Springer, Cham.
- [29] Vidya M.S., Patil M.C. (2019) , "Reviewing effectivity in security approaches towards strengthening internet architecture", International Journal of Electrical and Computer Engineering (IJECE) Vol.9, No.5, pp. 3862-3871 ISSN: 2088-8708, October 2019.

Author's Profile

	Vidya M S Completed B.E from Gulbarga University, M. Tech from VTU and pursuing PhD under VTU. Her area of Research is Network Security, and has teaching experience of 14 years. Published papers in National and International journals.
	Dr Mala C Patil completed B.E from Karnataka University, Dharwad, and M.S from bits Pilani and PhD from Anna University. She has teaching experience of 25 years. Her area of research is Software Engineering. She has Published papers in various national and international journals.
	Dr. Shiva Murthy G received the B.E. and M.E. degrees in computer science and engineering from Bangalore University, Bangalore, India. He received Ph.D. from National Institute of Technology Karnataka(NITK), Surathkal, India. His current research interests include wireless adhoc and sensor networks and IoT. Currently he is working as Associate Professor in the Dept of CSE, VTU Center for PG Studies, Muddenahalli.