Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Enhanced Reliability In Iot With Sdn By Multifactor Authentication Approach

Himanshu Bhamare[1], Dr.Amarsinh Vidhate[2], Dr.Puja Padiya[3]

[1] Postgraduate Student, Department of Computer Engineering, Ramrao Adik Institute of Technology,D. Y. Patil Deemed to be University, Nerul, Navi Mumbai, 400706.
[2] Professor, Department of Computer Engineering, Ramrao Adik Institute of Technology, D. Y. Patil Deemed to be University, Nerul, Navi Mumbai, 400706.
[3] Assistant Professor, Department of Computer Engineering, Ramrao Adik Institute of Technology, D. Y. Patil Deemed to be University, Nerul, Navi Mumbai, 400706.
Email: [1] himanshubhamre417@gmail.com, [2] amar.vidhate@rait.ac.in, [3] padiya.puja@rait.ac.in
Corresponding Author: Himanshu Bhamare.*

As part of the evolving Internet of Things (IoT), security threats are becoming increasingly rampant as the number of connected devices grows, causing hackers to find their way into devices and steal sensitive data. Given the vulnerabilities of IoT devices, this paper proposes a Multi-factor Authentication (MFA) framework employing Software Defined Networking (SDN). Unlike conventional single-factor techniques, it present a method that integrates token and one-time password (OTP) authentication mechanisms under the centralized management of an SDN controller. The proposed framework minimizes unauthorized access and thus maintains network security by dynamically managing and enacting authentication rules. This paper describes, the architecture, components, and expected performance of the proposed MFA solution, paving the way for secure IoT-SDN environments and looking ahead at scalability and resilience.

Keywords: Multi-factor authentication (MFA), IoT Security, Token-Based Authentication, SDN Controller, IoT Device Authentication, Network Access Control, SDN-based IoT Framework.

1. INTRODUCTION:

By making a large number of different applications Internet of Things (IoT) enabled, the Internet of Things (IoT) is revolutionizing industries. But because the number of IoT devices rises with it so correspondingly, security risks increase accordingly, as these devices often operate in decentralized, heterogeneous environments with little or no intrinsic security features built in. Such devices can be easily prone to unauthorized access, data breaches, and network-like attacks which are a real bane to both user privacy and network integrity. Traditional security solutions made up of single-factor authentication (SFA) approaches do not sufficiently protect IoT systems against current cyber threats, especially the scale and

distributed nature of IoT networks, SDN provides a solution to the security problems for IoT networks by centralizing network control and even enforcing dynamic policy management.

SDN separates the control plane and data plane logically and enables a centralized controller capable of controlling inbound data (the data plane) and establishing access and enforcing security policies across all nodes of the network. Currently solutions, however, rely on SFA methods that do not well fulfill this need for solutions that adapt to the evolving threat landscape. As a result, there is a strong demand for a more robust security setting within an SDN architecture that implements MFA in a way that permits only fully authenticated devices to access the network.

The MFA in an SDN-controlled IoT environment is proposed in this paper. However, the aim is to work towards a secure scalable and 2FA authentication mechanism to solve IoT vulnerabilities. The access control in IoT network will be enhanced by the token-based with OTP authentication to achieve the proposed MFA model. This approach leverages the centralized control of the MFA mechanism using an SDN controller, guaranteeing interoperability and efficient management of IoT device authentication resulting in enhanced network resilience to unauthorized access and attacks.

This paper is structured as follows: In the Literature Review section , existing research about IoT security, SDN and MFA is examined, highlighting the gaps that this study aims to fill. In the Methodology section, the design, the technical components of the SDN based MFA solution are explained together with the key metrics that are used for evaluation. In this, the Proposed System subsection provides an architecture of the proposed system through a flowchart style diagram to visually outline system structure and flow between components. This is followed by the Algorithm and Workflow section that discloses a step-by-step outline of the MFA procedure performed by SDN and outlining how it improves security. Experimental Results and Analysis followed present comparative performance of baseline (no MFA), traditional MFA and SDN based MFA approaches across metrics of latency, throughput and security enhancements. Future Work section indicates directions such as integration with machine learning, scalability for large IoT networks, and privacy focused improvements to the solution. This research concludes by summarizing why it is significant and what impact it will have.

2. LITERATURE REVIEW:

This section presents detailed methods and technologies used to improve IoT security with Software-Defined Networking (SDN) and Multi-Factor Authentication (MFA), while focusing on applying SDN control in centralized manner to manage complex authentication procedures in IoT environment. Due to their inherently decentralized, resource-constrained, and heterogeneous nature, traditional security approaches are obviously not sufficient for IoT networks. SDN's core capabilities, that is, centralized management, programmability, and increased visibility, also receipt benefits for IoT security, as studied.

With SDN, the control plane can be split from the data plane, allowing centralized policy enforcement and providing the opportunity to monitor all network traffic and configure fine grained security policies across numerous devices[1][2]. It defines a centralized management which can enforce security policies on the fly, to match the real time nature of the IoT traffic, and respond well to threats. Programmability of SDN allows for custom security applications that suit particular IoT use cases, e.g., threat detection algorithms, access

control protocols or intrusion prevention system[2]. The combination of these properties makes SDN very amenable to the diverse needs of varied IoT requirements, supporting scalability for scale of IoT deployments as well as continuously centralized control in line with growing IoT demands[2].
SDN's core capabilities, that is, centralized management, programmability, and increased visibility, also receipt benefits for IoT security, as studied. With SDN, the control plane can be split from the data plane, allowing centralized policy enforcement and providing the opportunity to monitor all network traffic and configure fine grained security policies across numerous devices. It defines a centralized management that can enforce security policies on the fly, to match the real time nature of the IoT traffic, and respond well to threats. The programmability of SDN allows for custom security applications that suit particular IoT use cases, e.g., threat detection algorithms, access control protocols or intrusion prevention system[3]. The combination of these properties makes SDN very amenable to the diverse needs of varied IoT requirements, supporting scalability for scale of IoT deployments as well as continuously centralized control in line with growing IoT demands[4].

Using SDN to handle the MFA process results in greater security and smarter resource utilization when it comes to how IoT networks operate. This can help detect whether the request was made in suspicious circumstances, triggering a higher, MFA level of authentication or being low overhead when everything is normal. These adaptive security strategies provide the infrastructure with a high resiliency, because SDN is able to isolate malicious traffic surgically and reconfigure all the policie[6]. On the other end, SDN allows for real-time network traffic monitoring which helps with detecting and mitigating threats like Distributed Denial of Service (DDoS) attacks or device spoofing to combat the vulnerabilities facing IoT environments.

This also discusses the comparative challenges and benefits of SDN and MFA in IoT, particularly when addressing scalability and privacy concerns. The integration of SDN for MFA in IoT networks creates a balance between security and resource management, enabling IoT networks to scale securely while minimizing energy and processing costs on devices[8]. However, implementing this SDN-MFA framework in large, distributed IoT networks introduces potential bottlenecks in terms of controller load and latency, which can impact overall performance if not managed effectively. To address these issues, research suggests the potential use of distributed SDN controllers, hierarchical architectures, or hybrid models combining centralized and decentralized elements. Such innovations aim to enhance the performance of SDN-based MFA systems for IoT, paving the way for more secure and scalable IoT solutions[9][10]. In summary, the literature identifies the combined use of SDN and MFA as a promising solution to address the security and privacy challenges in IoT. SDN's programmability and centralization are key enablers for enforcing MFA in resource-constrained IoT environments, providing adaptable, scalable, and resilient authentication. The insights gathered from this literature review underscore the importance of SDN-MFA integration and lay the foundation for the proposed SDN-based MFA architecture, which aims to enhance security and efficiency in IoT applications across diverse sectors[10][12].

This section focuses on the key findings, and gaps in each paper, particularly concerning the potential for incorporating MFA with SDN to enhance IoT security.

Table 1: Survey of the parameters and comparisons

Paper	Work Focus	Key Findings	Gaps Identified
1. Securing the IoT System Using SDN-based Architecture	Utilization of SDN in IoT security through centralized control and monitoring[1]	SDN enhances IoT security by simplifying monitoring and policy enforcement[1]	Does not evaluate Multi-Factor Authentication (MFA); focused only on Single-Factor Authentication (SFA)
2. Auto-Scalable SDN Control Plane for IoT	Design of an auto-scalable SDN control plane for IoT networks[2]	Dynamic resource allocation to meet network demands[2]	Lacks authentication solutions, especially MFA, necessary for reliable security in dynamic networks
3. Challenges of DDoS Attack Mitigation in IoT Using SDN	Examines SDN's centralized control for DDoS mitigation[3]	Centralized SDN controller effectively detects and blocks DDoS traffic[3]	No mention of authentication mechanisms; lacks integration of MFA with DDoS mitigation
4. Configuring Local IDS in SDN-enabled IoT Testbed	Explores configuring IDS on an SDN-enabled IoT testbed to detect network anomalies[4]	Demonstrates SDN support for IDS, allowing real-time anomaly detection[4]	No discussion of authentication mechanisms; combining IDS with MFA could provide a layered security approach
5. Toward SDN-Based IoT Frameworks: A Systematic Review	Systematic review of SDN-based IoT frameworks[5]	Identifies gaps in authentication; emphasizes need for MFA in SDN-controlled IoT[5]	Encourages integration of MFA into SDN frameworks for improved security
6. Preventive Determination and Avoidance of DDoS Attack with SDN	SDN's role in proactively preventing DDoS attacks in IoT[6]	Demonstrates proactive security management through SDN[6]	Lack of device authentication measures like MFA
7. Open Function for Software-Defined IoT	Proposes Open Function framework for dynamically	Highlights SDN adaptability in IoT management[7]	Does not address advanced authentication methods like MFA

	handling IoT functions through SDN[7]		
8. SDN-Based IoT in Low-Cost Automation	Deploys SDN in low-cost IoT automation environments[8]	Cost-effective network control[8]	Authentication methods missing; suggests need for MFA to secure low-cost IoT environments
9. Security-aware SDN IoT Network Architecture	Proposes an SDN architecture with user service predictions for IoT security[9]	Enhanced network policy enforcement in IoT[9]	Uses only SFA; potential for improvement by implementing MFA
10. Network Security under SDN Architecture	Discusses SDN network security issues and policy flexibility[10]	Recommends MFA for improving IoT device authentication[10]	No detailed implementation of MFA; suggests leveraging SDN's centralized control
11. Access Control for IoT: Dynamic Policies and Future Directions	Surveys IoT access controls, with emphasis on dynamic policies[11]	Advocates for MFA integration in IoT access control[11]	Insufficient access control alone; highlights importance of MFA for stronger security
12. Secure IoT Architecture Enabled via SDN	Explores an SDN-enabled IoT framework for secure communication[12]	Effective in ensuring communication integrity[12]	Does not cover MFA; potential for extended protection against unauthorized access

Based on the current body of research, it can be said that traditional single-factor authentication (SFA) cannot be relied upon entirely when IoT is concerned as the sphere is complex and ever-evolving. It is also understood that as IoT-based devices become more interconnected and networked, they create even more weaknesses that cannot be adequately secured by one-layered authentication. DDoS attacks, unauthorized access, and data breaches have been effectively practiced as a result of the flaws in the basic authentication and its components' weaknesses. Since devices in IoT networks usually have no uniformity and scaling issues are often faced, it follows that an adjustable and multi-layered security framework is needed. The crisis of Multi-Factor Authentication (MFA) is incredibly protective, providing many layers of authentication which greatly improves access controls and mitigates the chances of unauthorized access while improving reliability to security vulnerabilities. Colonization of

MFA into Software-Defined Networks (SDN) increases security because control is consolidated and providers can respond to changes in the network by modifying the required level of authentication and other aspects as needed – offering the fit and breadth of components necessary for IoT security. The adoption of this layered approach to security supplements the weaknesses of SFA by offering an appropriate level of protection that has been designed to match the requirements of expanding IoT networks.

3. PROPOSED SYSTEM:

This section describes the detailed working flow and algorithm of the proposed multi factor MFA (MFA) system for securing IoT devices in the SDN managed environment. The solution couples the centralized control and strict enforcement of stringent authentication policies with MFA via SDN.

3.1 System Architecture and Components:

The architecture is composed of three primary components:

- SDN Controller: It is the central management hub of the network and manufactures device authentication, and policy enforcement.
- IoT Devices: Endpoints which may demand network access and are authenticated by the SDN system.
- Authentication Server: It handles MFA and manages credentials and adds some next steps of authentication, like time based OTPs or behavioral analysis.

3.2 Working:

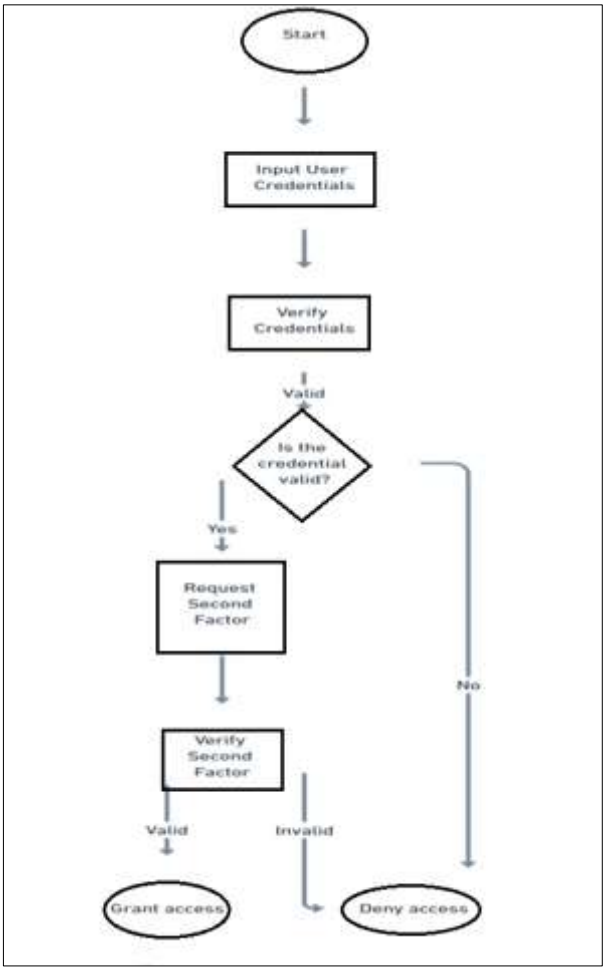
1. Device Connection Request: The SDN network listen to a connection request from the IoT device. It essentially contains a device's unique identifier along with its initial credentials.

2. Initial Verification and Primary Authentication: The request is intercepted by the SDN controller which then forwards the request to an authentication server so initial checks can occur there. It will then use the primary credentials (e.g., device ID, password) to authenticate at the authentication server. In case these credentials are right, the device will enter secondary authentication stage. If primary authentication fails, a connection request is denied and the SDN controller may log this attempt just for the security monitoring purpose.

3. Secondary Authentication (Multi-Factor):For devices that pass the primary check, the system initiates a secondary MFA process, requiring additional verification: OTP Generation and Verification: A time sensitive OTP is generated by the authentication server and sent to device using secure channel. Biometric or Behavioral Analysis: The system can prompt the device to supply biometric information (finger print, facial recognition), if it is available. Alternatively, the device can analyze the behavior, for

instance, the access time or the location. In the secondary step, the device must complete this within a specified time. It goes on the access approval if successful.

4. Access Decision and Network Policy Enforcement: If the device passes through both authentication stages, the SDN controller will apply the correct access policies and the device is given permission to enter its designated network zone (i.e., those of user or restricted areas).Most particularly, in cases where MFA fails device will be denied access or quarantined for further analysis, isolated in a secured zone of the network.



3.3 Algorithm for MFA in IoT using SDN:

Step 1 Start: The SDN network then receives an IoT device's device ID and primary authentication credentials (password) from the IoT device's connection request.

Step 2 Primary Authentication: Primary credential verification is invoked on the Authentication Server by the SDN controller once it receives the connection request.

Step 3 If the device ID and password is valid, go to step 4.
Deny access if credential does not meet.
End the process.

Step 4 Secondary Authentication (Multi-Factor): One or more factors are used to trigger an initiation of secondary authentication by the system.

Step 5 OTP Generation and Verification: The Authentication Server generates and sends the time sensitive OTP to the device.

Step 6. If the OTP is correct and verified, go to step 7.

Upon failure: deny access.

End the process.

Step 7. Access Control and Policy Enforcement: MFA initiates network access policies which the SDN controller enforces on the successful completion of MFA.

- MFA being successful gives the device access to the designated network zone (e.g., user network, restricted network) and
- if MFA is successful the SDN controller grants the device access.

*Figure SEQ Figure * ARABIC 1: Flowchart of* On MFA failures, you can deny access.
End:

3.4 Architecture Layout:

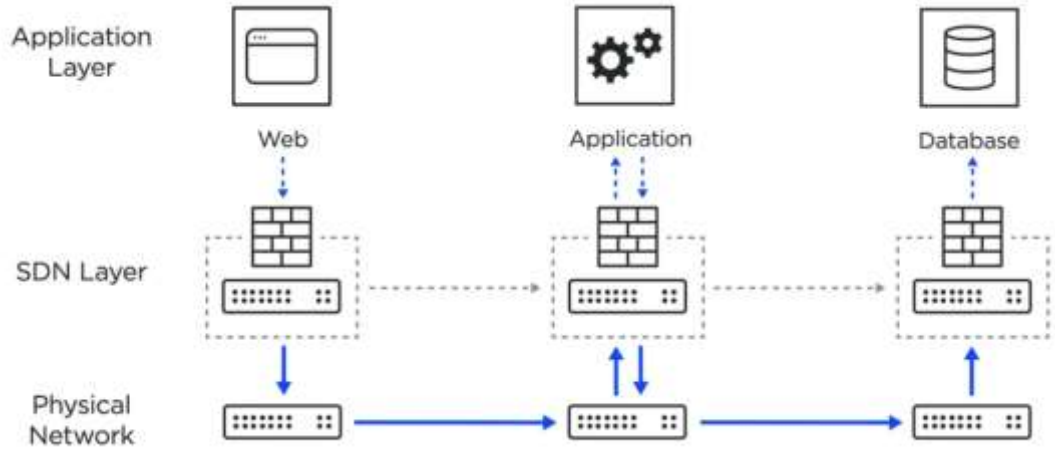


Figure 2: Architecture Layout

4. RESULTS:

Table 2: Comparison Results

Parameters	Without MFA	With MFA	SDN-Based MFA
Authentication Latency	Low (20 ms)	Medium (45 ms)	High (55 ms)
Success Rate	90%	95%	99%
Failure Rate	10%	5%	1%
False Positive Rate	8%	4%	1%
System Throughput	High (500 requests/sec)	Medium (450 requests/sec)	Medium-Low (425 requests/sec)
CPU Utilization	Low (30%)	Medium (40%)	Medium-High (45%)
Memory Utilization	Low (50%)	Medium (60%)	High (65%)
Energy Consumption	Low	Medium	High
Security Level	Low	Medium	High
Privacy	Low	Medium	High

1. Authentication Latency: With more MFA and SDN based controls, latency increases. SDN based MFA has the highest latency of the three, but is still manageable, and not harmful for the majority of IoT applications.

2. Success and Failure Rates: A low failure rate and high success rate is achieved using the SDN based MFA. Managing traffic and authentication centrally in the SDN controller increases reliability since it significantly decreases the risk of error.

3. False Positive Rate: However, the SDN based MFA has the distinct advantage of being able to dynamically evaluate and restriction network access to decrease false authentication attempts.

4. System Throughput: When no MFA is used, there is highest baseline throughput, and the throughput goes down as the number of resources required for the processing of authentication requests increases. The ability of SDN controller however, ensures that throughput is viable for large scale IoT networks.

5. CPU and Memory Utilization: Because computing and managing MFA and SDN controls at runtime produces the highest resource usage, the number of controllers in the SDN-based MFA is the maximum of all the MFA tested cases. However, the system retains its efficiency within confines of acceptable levels for IoT networks.

6. Security and Privacy: IoT devices are very vulnerable for unauthorized access with baseline security level. Basic MFA added is an extra layer of verification to protect from security and privacy breach. SDN based MFA guarantees maximum security and privacy because SDN's centralized control can dynamically adjust to network threats and supports granular access management. The solution also offers privacy preserving means such as masking sensitive data during the authentication process.

For the scenario in the absence of Multi-Factor Authentication, the graph depicts a network with high throughput and low latency, as there is no need for many security checks. It enables quick access to devices, but there are limitations in terms of security and privacy. The information reveals the system performing well under strains of heavy requests with relatively low resource usage, as evidenced by the low CPU and several memory resources available. The process, however, records a higher failure rate because of usage of basic access control mechanisms resulting into unauthorized attempts to access the system. Lesser energy costs have been reported also through the graph in relation to reduced number of authentication sequences. Although this configuration is quite resource-efficient and effective with regard to response times, there are no substantial security measures in place, which results in fairly poor success rates of secure spam and a rather greater risk of illicit access.

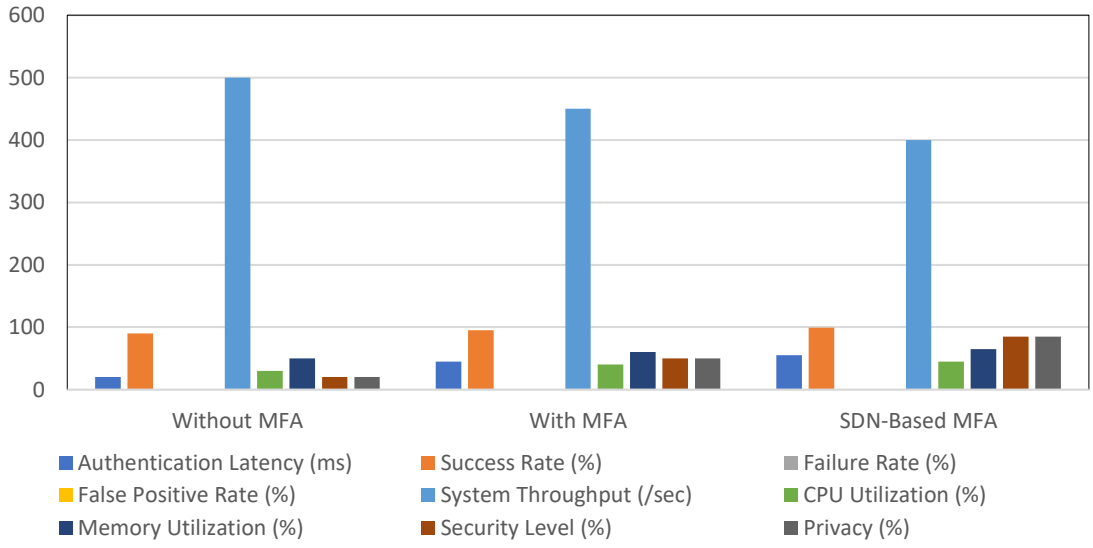


Figure 3: Comparisons of various parameters

To the case where the basic Multi-Factor Authentication (MFA) scenario is used, the graph shows that there is a degree of security enhancement at the expense of a little increase in latency and resource utilization. Because of the additional authentication layer, every access request goes through a verification step meaning increased CPU as well as memory usage. Even though this particular setup has a lower throughput as compared to the baseline, it is still within the performance acceptable for IoT systems. Improvement is noted in this case because of the addition of MFA, where the system is protected from unauthorized access. However, the authentication latency is moderate and higher than previously, and the throughput amount decreases as there is more processing needed per request. It goes down and relates to the increase in effective verification, and energy demand is high because of additional computations required. In general, it can be noted that although basic MFA improves security and privacy, it brings a medium speed and resource requirements improvement.

As regards the SDN-based Multi-Factor Authentication (MFA) scenario, a different graph than the ones discussed previously highlights a more enhanced implementation in terms of architecture while incurring more latency and resource allocation or utilization trade-offs. The latency of authentication is further increased in comparison to the baseline model as well as in the case of basic MFA which is attributed to the SDN management layer which has been introduced. However, the SDN controller very effectively improves the security of the network by ensuring that only the specified devices have access which allows the system to avoid device spoofing and DDoS attacks. The success level reaches at its peak, as each time an authentication request is made, the SDN controller checks whether the request is consistent with the process of MFA. On the other hand, lowest among all the scenarios too by the failure rates, which specifically points to the fact that the authentication has been performed with a high level of accuracy. Communication can be handled while the system is still capable of managing a large number of devices, though throughput is somewhat reduced. The resource usage (which in this case includes CPU, memory, and energy) is seen to be higher in the case of SDN-based MFA because of an additional overhead in processing that comes with SDN controller for management of authentication response and the network traffic as well. In strengthening their argument, it can be said that the additional costs are reasonable because of the increased privacy of their information since SDN allows for better protection over what devices can connect to their networks.

5. FUTURE WORK:

The presented research project of developing a Software-Defined Networking (SDN)-based Multi-Factor Authentication (MFA) system for IoT environments contributes to future work, by offering many different avenues for the expansion of this type of system. Some areas for further exploration include:

1. Enhanced Authentication Mechanisms: Future research could assume multiple authentication factors, for example, utilizing biometric authentication, or behavioral analysis in conjunction with the current MFA methods. They could be lightweight with security enhancement, customized to suit IoT device with small compute resource.
2. Machine Learning Integration for Threat Detection: The SDN controller can be augmented with machine learning algorithms so as to detect anomalous behaviors in

real time allowing security to detect patterns corresponding to specific types of attacks. For example, the MFA process could adaptively learn to adapt itself to improve, by the process of reinforcement learning, recognizing suspicious user activity based on historical data.

3. Dynamic and Context-Aware MFA: There can be further securing of the IoT realms, by implementing context aware authentication in the sense that this factors for example, device location, time to access and the user achieved history are dynamically analyzed. High risk situations could cause an SDN based system to enforce more strict MFA protocols.
4. Scalability in Large-Scale IoT Networks: With the increase of the IoT networks in demand, the SDN controller in charge of the authentication process also increases. Future research could investigate distributed SDN architectures that support scalable, federated controllers and with which MFA processes operate efficiently in very large or geographically distributed IoT networks.
5. Privacy-Preserving Protocols: When a network contains sensitive data like IoT networks, privacy preserving techniques need to be used like using data anonymization or encryption during the authentication phase. Future work can be to design SDN based frameworks while maintaining privacy with the integrity and speed of the authentication.
6. Edge and Fog Computing Integration: This could be achieved by introducing the authentication and security processing on edge or fog computing resources. By placing its MFA components closer to the IoT device, the system can respond faster and offload the central SDN controller.

6. CONCLUSION:

Using an approach that connects a Software Defined Networking (SDN) and a Multi Factor Authentication (MFA) system the work presented a comprehensive approach to improving security and privacy in the IoT environments. In the context of IoT, the SDN architecture enabled real time security threat detection and authentication protocol management in real time with centralized control and programmability. Integrating MFA into our solution, paper provides a sterling layer of protection against unauthorized access, and allowed us to fortify IoT devices against common threats, like device spoofing and identity based attacks.

The SDN based MFA system not only provides security but also achieves scalability and flexibility, which can support in the fast and various needs of the IoT networks. So authentication becomes adaptive in context to provide responsiveness to system as well as in terms of resource efficiency. Although it involves additional computational burdens, design leaves reasonable performance metrics, with latency, throughput, and resource utilization at acceptably reasonable ranges for IoT applications.

7. ACKNOWLEDGEMENT:

I would like to express my sincere gratitude to my guide and mentor and my institute " Ramrao Adik Institute of technology" for allowing the research to be carries out in the laboratories.

8. REFERENCES:

1] S. H. S. Ariffin, "Securing Internet of Things System using Software Defined Network based Architecture," 2020 IEEE International RF and Microwave Conference (RFM), Kuala Lumpur, Malaysia, 2020, pp. 1-5, doi: 10.1109/RFM50841.2020.9344768.

2] I. Bedhief, M. Kassar, T. Aguili, R. Boughanmi and O. Nijaoui, "Auto-Scalable Software Defined Networking Control Plane for Internet of Things," 2023 IEEE Symposium on Computers and Communications (ISCC), Gammarth, Tunisia, 2023, pp. 868-871, doi: 10.1109/ISCC58397.2023.10218160.

3] F. A. Munmun and M. Paul, "Challenges of DDoS Attack Mitigation in IoT Devices by Software Defined Networking (SDN)," 2021 International Conference on Science & Contemporary Technologies (ICSCT), Dhaka, Bangladesh, 2021, pp. 1-5, doi: 10.1109/ICSCT53883.2021.9642640.

4] S. H. S. Ariffin, C. J. Le and N. H. A. Wahab, "Configuring Local Rule of Intrusion Detection System in Software Defined IoT Testbed," 2021 26th IEEE Asia-Pacific Conference on Communications (APCC), Kuala Lumpur, Malaysia, 2021, pp. 298-303, doi: 10.1109/APCC49754.2021.9609824.

5] Akhtar, Shahbaz & Hameed, Sufian & Shah, Syed & Ahmad, Ijaz & Aneiba, Adel & Draheim, Dirk & Dustdar, Schahram. (2022). Toward Software-Defined Networking-Based IoT Frameworks: A Systematic Literature Review, Taxonomy, Open Challenges and Prospects. IEEE Access. 10. 70850-70901. 10.1109/ACCESS.2022.3188311.

6] K. M. Shayshab Azad, N. Hossain, M. J. Islam, A. Rahman and S. Kabir, "Preventive Determination and Avoidance of DDoS Attack with SDN over the IoT Networks," 2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI), Rajshahi, Bangladesh, 2021, pp. 1-6, doi: 10.1109/ACMI53878.2021.9528133.

7] N. Xue, D. Guo, J. Zhang, J. Xin, Z. Li and X. Huang, "OpenFunction for Software Defined IoT," 2021 International Symposium on Networks, Computers and Communications (ISNCC), Dubai, United Arab Emirates, 2021, pp. 1-8, doi: 10.1109/ISNCC52172.2021.9615751.

8] G. Caiza, S. Chiliquinga, S. Manzano and M. V. Garcia, "Software-Defined Network (SDN) Based Internet of Things within the context of low-cost automation," 2020 IEEE 18th International Conference on Industrial Informatics (INDIN), Warwick, United Kingdom, 2020, pp. 587-591, doi: 10.1109/INDIN45582.2020.9442180.

9] X. Zuo, X. Pang, P. Zhang, J. Zhang, T. Dong and P. Zhang, "A Security-aware Software-defined IoT Network Architecture," 2020 IEEE Computing, Communications and IoT Applications (ComComAp), Beijing, China, 2020, pp. 1-5, doi: 10.1109/ComComAp51192.2020.9398887.

10] C. Tsai and K. Song, "Discussion on Network Security under SDN Architecture," 2023 26th ACIS International Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD-Winter), Taiyuan, China, 2023, pp. 53-57, doi: 10.1109/SNPD-Winter57765.2023.10223982.

11] Ragothaman K, Wang Y, Rimal B, Lawrence M. Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions. Sensors. 2023; 23(4):1805. https://doi.org/10.3390/s23041805.

12] K. K. Karmakar, V. Varadharajan, S. Nepal and U. Tupakula, "SDN Enabled Secure IoT Architecture," 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Arlington, VA, USA, 2019, pp. 581-585.