*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10*
***Article Received:*** *26 August 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *02 November 2023*

# Hash based Mutual Authentication for IOT Networks

**Rohit Sharma[1], Kapil Kumar Kaswan[2]**
[1]Mtech Scholar, CSE Department, CDLU,Sirsa , India
rsrohitsharma206@gmail.com
[2]Assistant Professor, CSE Department, CDLU,Sirsa , India
kapilkaswan@gmail.com

**ABSTRACT-** Internet of Things (IoT) deals with the different types of devices/sensors/applications and it is quite challenging to secure the data transmission over IoT because anonymous users can join the network without authentication and network resources can be compromised. There is need to integrate authentication provision for IoT networks and in this paper, a mutual authentication based scheme will be introduced to achieve above discussed security goal and its performance will be introduced under different constraints (Throughput/energy consumption etc.)

**Keywords-** IoT, Network Security, Hash, Mutual Authentication, Cryptography

## I. INTRODUCTION

IoT enables the machine to machine based data exchange and it extends the capabilities of traditional networks. Data transmission over open environment may cause security breach as intruder can get the unauthorized access to network resources. Following are the basic security concerns as shown in figure 1.

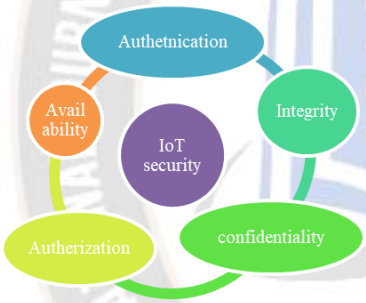


**Figure 1: Security concerns for IoT networks**

Figure 1 show the common security concerns for IoT networks such as authentication, authorization, availability/confidentiality/integrity of data.

All above discussed security concerns may differ w.r.t. IoT layers as given below:

- Threats for Application Layer: Denial of Services, Sniffing/ Phishing attack, Code injection
- Threats for Network layer: Sybill/sinkhole/man-in-middle attack
- Threats for Perception Layer: Spoofing, jamming, and cloning.

Following are the different security provisions w.r.t. different layers:

- Perception Layer: Authentication, Privacy, Risk Assessment
- Network Layer: Secure Routing, Intrusion detection
- Application layer: Cryptography, identity management

Security barriers for IoT networks are discussed below:

- IoT networks are low powered networks and lightweight cryptography algorithms are required to enforce the security provisions.
- Usage of shared network resources may invite the intruders.
- IoT networks operates over heterogeneous environment and It is quite complex to develop single security solution for different types of IoT devices.
- It is also complex to manage the identity of individual devices over network, as any device can join/leave the network at any time.
- IoT devices may be deployed over a large scale coverage area, it is quite difficult to ensure the physical security of IoT devices as intruders can damage the device or they can replace the original device with fake device.

Following are the possible solutions to incorporate the security provisions for IoT networks:

- A lightweight cryptography algorithm can be used to secure the data transmission
- Hardware level firewalls can be configured to block the unauthorized access to devices.
- Hardware locks can be configured with IoT devices during network deployment.
- Zero trust policy can be enforced to restrict the communication between devices. Only legitimate devices will be able to share the data over network. [1-5]

## II. LITERATURE SURVEY

Shilpa et al. [6] developed a solution to secure the communication over IoT network. It uses a lightweight cryptography algorithm to encrypt the messages for MQTT broker service. Analysis shows that it consumes optimal energy resources and it can guard the network against DNS level threats efficiently.

S. Roy et al. [7] proposed a multilayer security provision for IoT networks. It uses quantum cryptography algorithm for device authentication over network. Experiments show that it

outperforms under the constraints of compromised network as compared to existing schemes (RSA/ECC).

M. Alizadeh et al. [8] introduced a ticket based mutual authentication protocol for IoT Networks. Access to network resources is assigned as per the tickets issued to the end users. Analysis shows that it can prevent the different types of attacks i.e. denial of services/ impersonation etc.

Z. Wang et al. [9] used polynomial equations to authenticate the users over IoT networks. It verifies the users using equation generated data. Analysis shows that optimizes the cost of authentication as compared to existing schemes.

N. Doshi et al. [10] perfumed the cryptanalysis for various authentication protocols for IoT based networks. Study found that there are various constraints i.e. key generation over large scale networks, key distribution/management as well as verification of compromised keys over network and all of these factors are still open issues.

B. Hu et al. [11] introduced ECC based to factor authentication for IoT network security. Analysis shows that it offers reliable/secure communication at the optimal resource consumption as compared to existing schemes.

N. Odyuo et al. [12] proposed digital signatures based authentication scheme to recognize the IoT sensors over network. It uses two-factor authentication method to ensure the secure access to network resources. Experiments show that it is uses optimal energy consumption as compared to existing schemes.

S. Wang et al. [13] investigated the security issues for the IoT healthcare services. Study found that communication between gateway and end devices can be prone to the security threats and there is need to the secure commutation for intermediate devices. It also examined the various types of threats (i.e. session hijacking/brute force attack/false authentication etc.).

A. Y. F. Alsahlani et al. [14] presented a lightweight authentication scheme for cloud based IoT networks. It combines fuzzy logic with hash function to authenticate the users over network. Analysis indicates that it offers robust security for IoT devices as compared to existing schemes.

R. R. Pahlevi et al. [15] developed a two factor authentication scheme for IoT devices. At initial stage, all devices are registered and RFID based verification process is enforced to secure the transmission. Analysis shows that it can guard against sniffing threat and it has minimum false alarm ratio/error rate/false acceptance rate etc. as compared to existing schemes.

P. M. Chanal et al. [16] propped a regression based method to authenticate the IoT devices. As per request, session keys are produced and these are validated during transmission. Analysis shows that random forest classifier can be used to improve the accuracy of proposed scheme.

A. A. S. AlQahtani et al. [17] proposed a scheme to secure the IoT devices over ad hoc environment. It enforces access point based authentication to secure the transmission. Analysis shows that it consumes optimal resources and provides robust security as compared to traditional security provisions.

I. Ahmim et al. [18] presented a three factor based authentication scheme for IoT based intelligent transport system (ITS). It supports device authentication at highly mobile environment with optimal computational overhead as compared to existing ITS authentication scheme.

V. Iskandar et al. [19] used QR code based authentication for IoT based network. It uses advance encryption standard to ensure the secure communication. Analysis shows that it is compatible with Android devices and suitable for large scale networks.

B. Singh et al. [20] analyzed the security issues for IoT mobile application over cloud platform. Study shows that it is necessary to secure the intermediate devices along with cloud server. Researchers proposed a prototype to secure the data transmissions between IoT devices and cloud server. Experiments show that it ensures the secure communication over network using optimal resources.

## III. HASH BASED MUTUAL AUTHENTICATION FOR IOT NETWORKS

Member Node *MN*
Gateway *GW*
Step 1: IntializeIoT network
Step 2: Configure gateway(s) Gw
Step3: Generate hash (Server, ∑GW)
Step: 4 Assign (hash, ∑GW)
Step 5: Generate hash (GW, ∑MN)
Step: 6 Assign (hash, GW, ∑MN)
Step 7: Authenticate (∑GW, Server)
Step 8: Authenticate (∑GW, ∑MN)
Step 9: Start transmission
Step 10 MN->Encrypt (MN ->message, MN->key)
Step 11 MN->(hash, message, GW)
Gateway Side message receiving:
Step 1GW->verify (MN-MSG, hash)
Step 2: If MN->hash==true GW->forward(MN->msg, server, GW->hash)
Server Side message receiving
Step1: Server->verify(MN-MSG, GW->hash)
Step 2: If GW->hash==true Server->accept(GW->msg, GW->hash)

First of all, server generates a default hash code and keys to be assigned to the intermediate gateways and member nodes. All Gateways receive these and further distribute to the member nodes.

These hash codes are used to communicate with the intermediate gateways. To forward the data to gateway, messages are encrypted using keys and a hash code is embedded to ensure the integrity of the messages.

After receiving the data from member nodes, its integrity is verified by the Gateway and the messages having valid hash codes are forwarded to server side. Gateway cannot decrypt the intermediate messages.

At server side, hash code of the gateway is verified and data having valid hash code is accepted and decrypted at server side only. Intermediate gateways cannot decrypt the incoming data.

Server can update the keys and hash codes for gateways/member nodes.

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 10*
***Article Received:*** *26 August 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *02 November 2023*

Gateway performs authentication of intermediate nodes using their valid keys and hash codes as well as intermediate nodes can also verify the hash codes of the gateways before transmission.

In case of compromised network, nodes with invalid hash codes are isolated from network. Server is responsible to authenticate the gateways on the behalf of gateway's keys and hash codes.

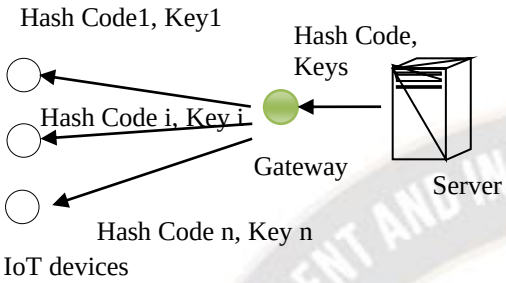


**Figure: 2 hash code and keys distribution**

Figure: 2 shows that server generates the unique hash code and keys for each node/gateway and distribute these to the gateways and gateways are responsible to distribute the hash codes and keys to individual member node. During transmission, has codes of nodes/gateway are verified to ensure the authenticity as shown on figure: 3.

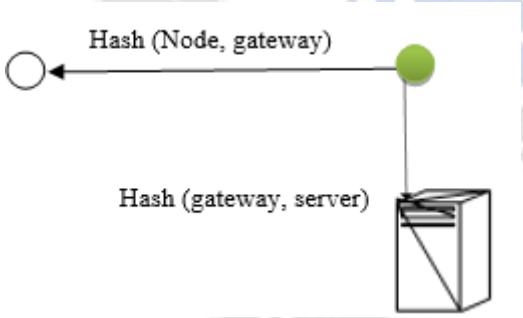


**Figure: 3 Authentication between m=nodes/gateways/server**

## IV. RESULTS AND ANALYSIS

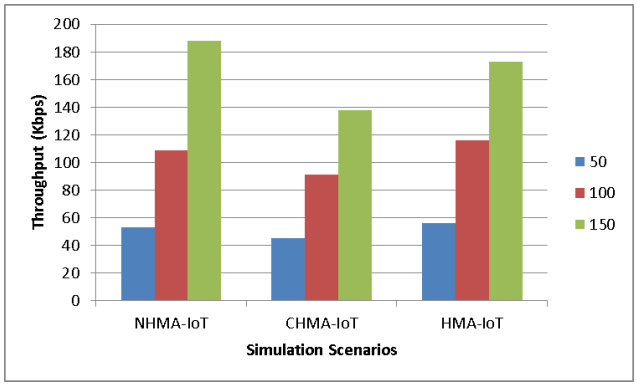


**Figure:4 Throughput**

Figure4 shows the throughput of the different scenarios. In case of NHMA, its value is at normal level but in case of compromised network, it is decreased and it is enhanced using HMA scheme.

Using NHMA scheme, in case of 50 node density, throughput is 53Kbps, for 100 nodes, it is 109Kbps and with 150 nodes, it reaches up to 188Kbps.

With CHMA scheme, In case of 50 node density, throughput is 45Kbps, for 100 nodes, it is 91Kbps and with 150 nodes, it reaches up to 138Kbps.

Using NHMA scheme, In case of 50 node density, throughput is 56Kbps, for 100 nodes, it is 116Kbps and with 150 nodes, it reaches up to 173Kbps.

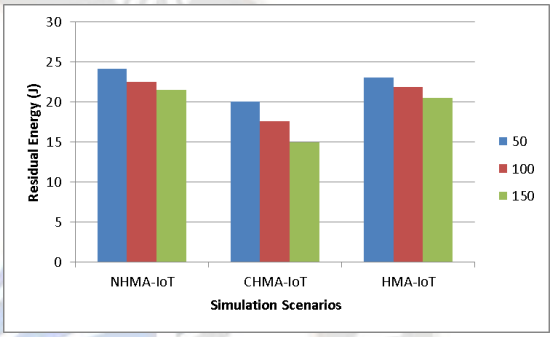


**Figure 5 Residual Energy**

Figure 5 shows the residual energy of different simulation scenarios. It can be observed that it is varying w.r.t. each scenario. With minimum sensor density, it is at peak value and it is declined as the sensor density varies from 100 to 150 sensors w.r.t. each scheme.

Using NHMA scheme, In case of 50 node density, residual energy is 24.1142J, for 100 nodes, it is 22.4658J and with 150 nodes, it is declined up to 21.4797J.

With CHMA scheme, In case of 50 node density, residual energy is 20.0042J, for 100 nodes, it is 17.5942J and with 150 nodes, it is declined up to 14.9846J.

Using NHMA scheme, In case of 50 node density, residual energy is 23.0242J, for 100 nodes, it is 21.8658J and with 150 nodes, it is declined up to 20.4797J.

## V. CONCLUSION

In this paper, a mutual authentication based security provision was introduced that uses multiple hash to secure the communication between end devices and gateways as well as it also secures the communication between intermediate gateways and server. Its performance was also analyzed using different parameters i.e. Throughput/residual energy etc. under the constraints of sensor density variations.

In case of NHMA, network delivered highest Throughput with acceptable energy consumption and there are little bit variations in these values.

In case of CHMA, throughput is declined w.r.t. node density as well as residual energy also varied. However in case of HMA, it can be observed that it maintained the highest throughput and residual energy w.r.t. node's density.

As per the analysis, it can be concluded that proposed scheme improved the overall performance of the network and in future, it will be further implemented to secure the other network types (i.e. Wireless sensor networks/ vehicular ad hoc networks etc.)

**REFERENCES**

[1] K. K. S. Gautam, R. Kumar, R. Yadav, P. Sharma, "Investigation of the Internet of Things (IoT) Security and Privacy Issues", 5th International Conference on Inventive Research in Computing Applications, IEEE-2023, pp.1489-1494.

[2] J. Singh, G. Singh, S. Negi, "Evaluating Security Principals and Technologies to Overcome Security Threats in IoT World," 2023 2nd International Conference on Applied Artificial Intelligence and Computing, IEEE-2023, pp.1405-1410.

[3] S. Kumar, A. Vidhate, "Issues and Future Trends in IoT Security using Blockchain: A Review," 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things, IEEE-2023, pp.976-984.

[4] D. S. Tundalwar, R. A. Pandhare, M. A. Digalwar, "A Taxonomy of IoT Security Attacks and Emerging Solutions", 2nd International Conference on Paradigm Shifts in Communications Embedded Systems, Machine Learning and Signal Processing,IEEE-2023, pp. 1-5.

[5] R. Veluvarthi, A. Rameswarapu, K. V. SaiKalyan, J. Piri, B. Acharya, "Security and Privacy Threats of IoT Devices: A & Short Review," 2023 4th International Conference on Signal Processing and Communication, IEEE-2023, pp. 32-37.

[6] Shilpa, Vidya A, S. Pattar,"MQTT based Secure Transport Layer Communication for Mutual Authentication in IoT Network, Global Transitions Proceedings, Vol. 3, (1), Elsevier-2022, pp.60-66.

[7] S. Roy, S. Deb, H. K. Kalita, "A novel hybrid authentication protocol utilizing lattice-based cryptography for IoT devices in fog networks", Digital Communications and Networks, Elsevier-2022,pp.1-16.

[8] M. Alizadeh, M. H. Tadayon, A. Jolfaei, "Secure ticket-based authentication method for IoT applications", Digital Communications and Networks, Vol.9, (3), Elsevier-2023, pp.710-716.

[9] Z. Wang, J. Huang, K. Miao, X. Lv, Y. Chen, B. Su, L. Liu, M. Han, "Lightweight zero-knowledge authentication scheme for IoT embedded devices", Computer Networks, Vol. 236, Elsevier- 2023,pp.1-20.

[10] N. Doshi, P. Chaudhari, "Cryptanalysis of Authentication Protocol for Cloud Assisted IoT Environment", Procedia Computer Science, Vol. 220, Elsevier-2023, pp.886-891.

[11] B. Hu, W. Tang, Q. Xie, "A two-factor security authentication scheme for wireless sensor networks in IoT environments", Neurocomputin, Vol.500, Elsevier-2022, pp.741-749.

[12] N. Odyuo, S. Lodh, S. Walling, "Multifactor Mutual Authentication of IoT Devices and Server", 5th International Conference on Smart Systems and Inventive Technology, IEEE-2023, pp.391-396.

[13] S. Wang, X. Zhou, K. Wen, B. Weng, P. Zeng, "Security Analysis of a User Authentication Scheme for IoT-Based Healthcare", IEEE Internet of Things Journal, Vol.10 (7), IEEE- 2023, pp. 6527-6530.

[14] A. Y. F. Alsahlani, A. Popa,"LMAAS-IoT: Lightweight multi-factor authentication and authorization scheme for real-time data access in IoT cloud-based environment", Journal of Network and Computer Applications, Vol.192, Elsevier-2021, pp.1-25.

[15] R. R. Pahlevi, V. Suryani, H. H. Nuha, R. Yasirandi, "Secure Two-Factor Authentication for IoT Device," 2022 10th International Conference on Information and Communication Technology, 2022, pp. 407-412.

[16] P. M. Chanal, M. S. Kakkasageri, "Random Forest Algorithm based Device Authentication in IoT," 2023 IEEE International Conference on Electronics, Computing and Communication Technologies, IEEE-2023, pp.1-6.

[17] A. A. S. AlQahtani, H. Alamleh, B. Al Smadi, "IoT Devices Proximity Authentication In Ad Hoc Network Environment," 2022 IEEE International IOT, Electronics and Mechatronics Conference, IEEE-2022, pp. 1-5.

[18] I. Ahmim, N. Ghoualmi-Zine, F. Bouakkaz, A. Rachedi, "Enhancement of a User Authentication Scheme for Big Data Collection in IoT-Based Intelligent Transportation System", 10th International Conference on Wireless Networks and Mobile Communications, IEEE-2023,pp.1-6.

[19] V. Iskandar, V. Mappadang, F. Dewanta, H. Nuha, "An Authentication Scheme for IoT-Based Mechanical Relay Utilizing QR-Code and MQTT", IEEE Asia Pacific Conference on Wireless and Mobile, IEEE-2023, pp.278-283.

[20] B. Singh, R. Lal and S. Singla, "A Secure Authentication mechanism for accessing IoT devices through Mobile App", International Conference on Computational Modelling, Simulation and Optimization, IEEE-2022, pp.274-278.