International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

An Authentication Scheme for an IoT Environment using Advanced Multiple Encryption System

M. Sundarrajan, A.E. Narayanan

Abstract: ***Internet of Things (IoT) has become one of the most important fields of research as it plays a vital role in performing an assigned task with various smart devices. These connected devices work together to achieve a common goal. Numerous researchers have been working in various sectors of IoT for obtaining a betterment in the entire function of an IoT environment. Securing the data being transmitted or stored in these smart devices in one of the major fields of research. Some of the security challenges faced in an IoT environment are in the areas of user authentication, user privacy, access control, information confidentiality, trust, mobile security and policy enforcement. To overcome all these challenges. In this paper, we have proposed a system called*** *AMES (Advanced Multiple* ***Encryption System) which also secures the overall communication of the network. The paper briefs an overview of an IoT environment, consisting of some hackers where the user connection with the controller is blocked without the presence of integrity and confidentiality. The paper also discusses the various security benefits of RSA and SHA. The proposed AMES system is based on Hardy Wall Algorithm and MQTT protocol. The differentiation of the proposed protocol and HTTP protocol is stated clearly The experimental results are obtained for the proposed authentication scheme using NS3 simulator by showing the comparison between existing hybrid security system with our proposed authentication system. The results also state that the designed AMES authentication system using MQTT protocol can minimize the level of security threats and other complications in transmission of the data in IoT environment.***

Keywords **: *Advanced*** *multiple* ***encryption System, MQTT, Internet of Things, Authentication, Security***

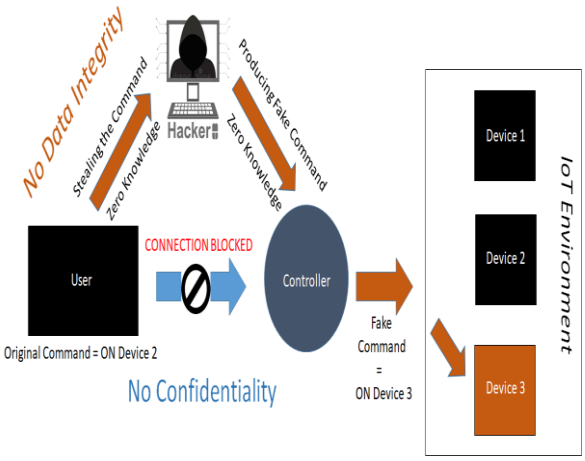
I. INTRODUCTION

IoT device security plays a main role in the networking environment. IoT acts as a connection between virtual and physical world that establishes our quality of our life. Here IoT security can be well-defined as a technological area alarmed with the protection of associated devices and networks in the Internet of Things (IoT). It provides a system of interconnected computing devices with the help of internet connection, digital and mechanical machines, objects, people etc.

Revised Manuscript Received on November 30, 2019.
***** Correspondence Author
M.Sundarrajan*, Department of Computer Science and Engineering, Periyar Maniammai Institute of Science & Technology, Thanjavur, India.
A.E.Narayanan, Department of Computer Science and Engineering, Periyar Maniammai Institute of Science & Technology, Thanjavur, India.

Here every object is provided with a unique identifier and also with the capability of transmission of data over a network automatically. When we permit these devices to associate to the open internet then they are open to a wide variety of severe liabilities and we need protection for that. Our suggested scheme uses X.509 certificate that uses a public key infrastructure (PKI) standard to authenticate whether the public key belongs to the computer or user or other service identity present within the certificate. We also utilize RSA security method. It is the most adaptive authentication scheme used by millions of users to provide fast business driven approach to integrating technologies. When it is added into the system, users should provide their RSA ID during the authentication phase within the time limit else the ID changes. From this users can have a secured connection over the interconnected networks. We also use SHA (Secure Hash Algorithm) to provide cryptographic computer security. It provides a hash value to security and encryption of data object. There are many protocols that used SHA such as TLS, SSL, PGP, SSH, MIME and IPSec. When many devices are connected in the IoT environment there are possibilities for security breach. In a case when the user provides an original command 'On Device 2' to the controller, the original message from the user is hacked and the controller receives only the fake command 'ON Device 3'. Here the connection is completely blocked or breached by the hackers and hence there will be no confidentiality. Hackers are certainly stealing the user's original command without their knowledge. User will have zero knowledge about the circumstance and that's a great benefit for the hackers. Here the data integrity is completely abandoned. Now the hacker will produce a fake command and will direct that to the controller. Controller also has zero knowledge about the circumstance and it will proceed with the processing phase with the received fake command. Now the entire processed information will be delivered to the device present in the IoT environment. This entire security breach is depicted in Fig. 1, where user sends a unique command to the controller but that connection is blocked by the hacker. The hacker will create a false command and transfer it to the receiver end. The user and the controller will have zero knowledge about it and the entire IoT environment is breached with security. In order to make the connection between the user and the controller in all devices in the IoT environment secure, our proposed scheme uses RSA, SHA and X.509 authentication scheme to provide a secured connection in the IoT environment. We also use a secured MQTT protocol instead of HTTP since it is slow and deliver more overhead compared to MQTT.

We use AMES encryption system for secured way of communication in the IoT environment.



Formulation and algorithm of AMES is mentioned in our methodology segment and we have evaluated the performance as well with a comparison of the existing hybrid security system and our AMES security system.

Fig. 1 - Combinations of X.509, RSA and SHA Security Benefits

II. LITERATURE SURVEY

We have referred numerous research materials to identify the current and previous methodologies followed to improve network security in the IoT environment. All the referenced materials are mentioned here as follows. Alcaraz C in [1] observes that many industries are revolutionizing its critical systems to move forward with the upcoming industrial revolution. IIOT is considered as one of the highest applicable technologies of today's world. The author suggested that with the help of IIOT industries can effectively handle the extensive controls, possibility of monitoring from any place and any time in an effective way. In [2], they have proposed a secured framework with low complication to provide secured communication and protected authentication in the IoT environment. A distinctive user identity is developed with the help of unique radio frequency fingerprint technology. They are manipulating the wireless channels present in between the source and the destination as cryptographic keys. This methodology is applied to the network protocol's physical layer. In [3], their proposed methodology uses CoAP that will make the clients monitor the resources present in the server in an energy efficient way. They also use AES with 128 bits key length to create a secured network session. Their scheme is very much efficient, less network connection overhead, providing a defense mechanism for attacks like denial of service, tampering, exhaustion of resources etc. In [4], they have developed a peculiar security mechanism for the IoT system by finding out the major threats in every module of the system and they are minimizing them as well in the same phase. There will be many restrictions for smart toy's hardware so they have presented a specific encryption methodology that proved to provide secure solution for the sensitive IoT environment. In [5], they have proposed a methodology with three phases of security. The first phase handles non interfered messages of light weight data. The next phase increases the privacy of data in both source and destination level. The last phase will provide a security for a longer term with reciprocated authentication. They have also used MQTT security framework supporting cryptographic schemes. In [6], they have discussed about the current protocol standards for cryptographic schemes that are widely used in the IoT devices. They have analyzed the strength and weaknesses of the cryptographic standards by comparing it with variety of areas such as smart home, health, consumer devices etc. Out of all these they also deliberate about the upcoming challenges faced by the IoT in future world. In [7], here they focus on the critical IoT components and the security necessities at the perception layer. They emphasis on RFID and sensor network at this layer and classify variety of attacks via taxonomic grouping and they deliberate the required solution. At the end they work on the perception layer challenges and finding appropriate rectifications effectively.

In [8], here they utilize a cryptographic technique to provide encryption to personal data obtained from various medical sources. They embed the data encrypted and convert them into a low complexity image with the help of XOR stenography encoding methodology. They also use adaptive firefly algorithm to provide optimization to the certain image blocks. At the final stage the hidden data in the image is decrypted and recovered. In [9], here they suggest a novel secured authentication scheme for heterogeneous IoT in order to shift between PKI and CLC environment. The suggested scheme can guarantee the authorized users by providing secured communication. This scheme will also support other attributes like non repudiation, user anonymity etc. The proposed scheme proved the resistance of DOS attack and replay attacks. The methodology is also lightweight and advanced approach. In [10], firstly they offer a horizontal overview of block chain mechanism. It is in good relation with other growing technologies such as IoHT, IoE, IoC, blockchain and IoV. Every subsector in the IoT environment gives a brief comparison over blockchain mechanism with security measures, performance, complexity etc. The main aim of this paper is to provide a summary of all the block chain protocols especially designed for IoT environment. Sundarrajan and Narayanan in [11] have proposed a model called Hardy Security System which will secure the Device ID instead of the transmitted data. They utilize Fermat's theorem and the steps involved is also discussed clearly. They also utilize advanced multiple cryptology to reduce the security threats. The suggested methods have reduced the data leak up to 20% and the communication bandwidth also decreased to 3% from 5%. They use NS2 simulator to evaluate the performance of the suggested model and that gave less memory consumption, less fake ID usage, safer system etc.

In [12], they utilize an optimized innovative cryptographic model to examine the safety of medical images. They store the data of the patients in the cloud to make it vivacious. Using grasshopper optimization and particle swarm optimization the security level of encryption and decryption is increased. The optimal key will also be selected these two optimization schemes. The evaluated results are finest compared with the existing schemes. In [13], they make a survey about IoT security framework by considering eight frameworks. They simplify the proposed architecture, smart apps and compatible hardware for each framework and also by providing other security properties. In [14], they discuss about the target of cyber-attacks by how the IoT environment is open to all and possessing high processing power. Here they present the current foremost forensic and security challenges in IoT domain. They have also mentioned about other published papers related to their identified challenges. In [15], they have presented a novel and systemic approach to the security challenges faced in the IoT environment. The role of each component is clearly mentioned and explained. They have presented a case study about its interactions and impact with the other main components. Various research challenges are highlighted based on the novel taxonomy of the IoT framework. In [16], at first they establish quantum computer's impact on the cryptography security scheme utilized today. They also gave an outline for the same for both quantum and classical computers. They provide the implementations and overview for ongoing cryptographic project schemes that will provide solutions for the future security development for IoT. In [17], they deliberate about networking devices that are in usage of IoT are of low energy and lightweight. Such devices should dedicate their maximum available energy and computation to working core application functionality. Thus it makes the security and the privacy of the user data relatively challenging.

In [18], they converse about the security necessities of RFID authentication scheme. They provide a brief review of ECC-based RFID authentication scheme in both security and performance factors. They also discuss about the three major ECC based authentication scheme based on performance and security factor appropriate for healthcare environment. In [19], they suggest a XOR manipulation scheme based on encryption methodology rather than the usage of complex encryption methodologies. The complete enhancement of the security protection is well described. Hardware design approach is also mentioned clearly. Li and Xiong in [20] propose an online and offline encryption scheme to provide safe and secure communication between the host and the sensor node in a network. Their proposed methodology is indistinguishable compared with other cipher text attacks and adaptive chosen message attacks. Their scheme provides more privacy, achieves authentication and more reliability. In a public key infrastructure, this methodology will allow a sensor node to deliver a message in the internet based on identity cryptography method. During offline phase, substantial computations are done without the knowledge of the message and during online phase, insubstantial computations are done when the message is available. To integrate WSN to IoT their methodology works well for a perfect solution to the security threats.

In [21], in order to address the issues related to cyber security they present various security approaches based on cyber entity activity cycle by considering U2IoT approach. The proposed system offers a solution to the challenges faced by the researchers so far based on network security, application security and system security. In [22], they propose architecture named OSCAR that will provide end to end object based security for IoT environment. It comprises authorization servers that will give secret access codes to clients which will make them to request essential resources from CoAP nodes only. A reply will be sent from the CoAP nodes for the requested resources. This methodology supports network traffic and catching as well. They have evaluated the OSCAR based on LLN and M2M communication using MAC layers and Cooja emulator. The evaluated results outperform the DTLS's security schemes even when the number of nodes is increased.

In [23], this paper discussed about security challenges and attacks of ransomware in IoT environment. They categorize and classify the works based on current technologies, necessities, IEEE standards, threats etc. They also itemize the requirements that are essential for a secured IoT environment. Various crucial open research challenges are recognized and deliberated. Thus they provide a brief overview of all the security challenges faced by the IoT effectively. Sahraoui and Bilami [24] propose a 6LoWPAN compression for the header of HIP packets. They also suggest an adaptive distribution security computational load system in HIP – BEX. They combine both E2E and HIP in IoT to attain end to end security. After evaluation the suggested solution CD – HIP is energy efficient and compatible with standard HIP. In [25], they propose network architecture with more security with key distribution mechanism with the help of automated and local authorization entities. They address various IoT related issues by including resource constraints as well. After evaluation the suggested model's overhead rate scales at a considerably slower rate in comparison with TLS and it also works well with resource constrained devices. In [26], they explore various networking technologies in IoT environment related to routing protocols and encapsulation. They provide a layer based taxonomy and explained how the network protocols will operate and fit with the current IoT requirements. Various networking issues such as interoperability, compatibility and issues related to configuration of existing and emerging protocols. They have implemented all this with the help of IPV6.

In [27], they propose an effective mechanism that will smart object in their life cycle based on authentication and authorization. The suggested methodology is acquiescent with architectural reference model provided by EU EP7 IoT-A project. Thus they provide a lightweight authentication smart object framework.

In [28], in this paper they suggest a protocol with the help of ECC to verify the reader's identity before providing the certificate that will provide user authentication and allows them to use the cloud interface in RFID environment. In [29], here they discuss about the security issues that will arise when the network interactions increase in IoT environment. They completely focus on U2IoT framework to design APHA based on layered networks. Firstly, the combined proofs are recognized for multiple targets to attain forward and backward transmission of data. Secondly, homomorphism, path descriptors and chebyshev maps are applied together for mutual authentication. Finally, various access authorities are allotted to attain hierarchical control of access. The proposed APHA has nil security defects and it's available for IoT and U2IoT applications. In [30], they present a highly optimized ECC for Tmote and MICAz sky nodes. It will support signature schemes and key exchange. Their elliptical curve implementation supports pseudo mersenne prime fields with two optimized designs HS and ME version. They also evaluate their model for energy consumption criteria during timing and SAP attacks. In [31], they suggest an efficient data collection method related to authentication system requirements. The suggested work will significantly contribute to the upcoming industrial IoT methodologies in an effective manner. They even perform a multiple analysis of their model in an optimized way. The suggested model's efficiency is evaluated through numerical results.

III. METHODOLOGY

The proposed IoT based AMES encryption model's device management; communication security and connectivity speed are evidently described in this module. We successfully provide protection to the entire user id's and device ids of all the IoT devices with the help of hardy wall encryption algorithm. With the assistance of this algorithm the communication bandwidth can be effectively decreased and will provide minimal memory consumption. We have used this algorithm between the IoT environment and the devices mainly for secured transmission of messages and also to avoid data leaks. In order to send all the messages securely we utilize MQTT (MQ Telemetry Transport) protocol. It keeps the flag alive, exceptionally lightweight, more scalability, less consumption of network bandwidth, effective distribution of information etc. It can even transmit the data over long distances without altering any routes in the network. That's why it is very well suitable for IoT environment. In a comparison to HTTP, MQTT is faster because it utilizes smaller data packets to communicate with the server, less overhead because it always keeps the connection online and makes an open channel between broker and the client, less power consumption since it uses smaller packets than HTTP. In order to provide symmetric encryption to our suggested model we utilize an advanced multiple encryption system for a secured communication. Advanced constrained devices are present within an IoT environment. Here all the devices are mainly controlled by IoT. When a communication or booting process takes place, it will happen only when the devices are enclosed in an IoT environment. AMES provides increased communication security to these advanced IoT environment devices. The entire network information is protected by secured keys and also with the help of secured protocols. An encryption mechanism is applied during the user authentication phase before the network communication begins. This is done with the help of hardy wall encryption mechanism. In Fig.2, our proposed architecture is diagrammatically represented. Here in the first phase, user enters their user id and password via user authentication phase in their personal computers or laptops. The password and the user id are effectively encrypted with the help of hardy wall encryption algorithm. At this phase hacker cannot steal the user credentials since it is entirely encoded. In the second phase, the request has to be securely transferred to the server in spite of the encryption since there should not be any loss of packets or any breakages in the message sent. With the help of our secured MQTT protocol the message is transmitted to the receiver with the help of a secured key protection mechanism. The entire message is bounded with private key lock protection. At the last phase, using AMEs secured communication mechanism the original message is now been received at the receiver end in an IoT environment without any data leaks. The broker or the server will now decode the original message and serve the response in an effective way. Thus through our proposed architecture, the network communication takes place without any delay in the response. Since the messages are sent via small packets of information, the communication speed in the network is efficiently increased and overhead is also very less. This is what is required in our today's world with an emerging IoT environment.

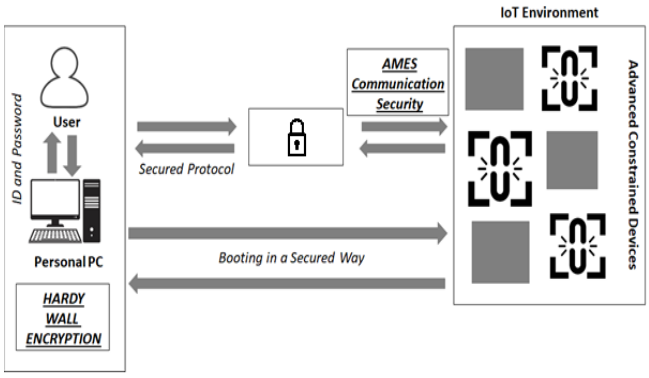


Fig. 2 – AMES in IoT Environment

Formulation and algorithm:

We utilize an AMES encryption algorithm. Here the input will be the encrypted formula and then an advanced multiple formula will be created with parameters 'E', 'W' and 'S'. For each created formula a new AMES formula will be generated. We have set a condition here where, when a generated AMES formula is able to add with the created multiple formula then the network communication will be initialized. If not then there won't be any communication and a notification will be sent regarding the same.

Thus the final outcome will be secured data communication. The algorithm is mentioned as follows.

Input: *Encrypted formula*
Create a *Advanced Multiple Formula* to *E(W,S)*
for each *Encrypted formula E(W,S)* **do**
  Generate *Formula AMES*
  Add *Formula AMES* with *E(W,S)*
end for
If *Formula AMES* is added with *E(W,S)*
  Initialise the communication
else
  Stop and Notify
end if
Output the Secured Data Communication

AMES Formula:

The AMES formula is the combination of data or command parameter, key usage restriction parameter based on sequence number and the last parameter will be the private key. Along with this formula, the created multiple formula with the parameters 'E', 'W' and 'S' denoted as 'HW' is added here. The stated AMEs formula is mentioned as follows.

AMES= Data / Command + key usage restriction with sequence number + private key

$$AMES = D+KR+PK$$

Where:
D *- Data / Command*
KR *- key usage restriction with sequence number*
PK *- private key*
Finally, by adding module 1,

$$AMES = D+KR+PK+HW$$

Where:
HW *- E(W,S)*

IV. RESULT EVALUATION

We have evaluated our proposed model on two bases. We have assessed the dataset by checking the performance of the data with the help of applications. We also evaluated the dataset by checking its communication performance with the help of NS3 simulator and by means of table as well. From the evaluate results we can identify that the number of attackers are greatly reduced. The energy consumption level is also very low and the level of security is greatly increased. In Fig. 3, with the help of an application, a new network connection is added with the parameters connection name, client ID, broker web address, port number, network protocol, connection time out, keep alive status, username and password. When the connection is enabled we can able to control other appliances such as switches, fan, etc., and also temperature level, humidity level, radio etc. The entire progress level can be monitored and we can have our button controls as well. All these are displayed in ESP 8266 section of the application. We can able to see the status of temperature level of the living room, office, kitchen, dining, outdoor etc., in the status section of the application.

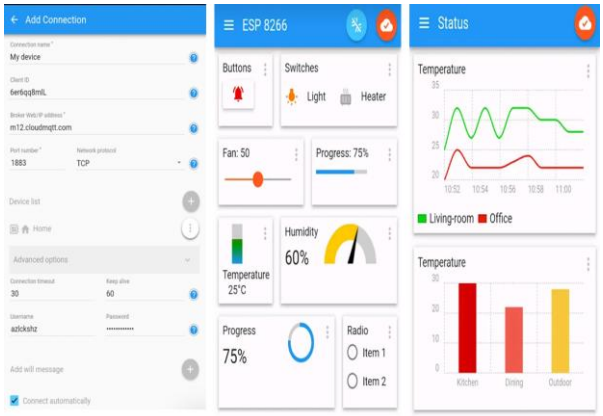


Fig. 3 – Application Based AMES Authentication

In fig. 4, the level of security is evaluated for our proposed AMES system (indicated by red color), existing hybrid security system (indicated by gray color) and cryptographic algorithmic combination systems (indicated by green color). The security level is indicated from value '0' to '100'. The number of security models is indicated from value '0' to '90'. The maximum level of security is reached by the AMES system at the security level '80'. The second highest security level is reached at the level '60' by the existing hybrid security system. The least security level is provided by the cryptographic models at the security level of '30'

In Fig. 5, the energy level comparison is made for AMES security models and other security models. Here the energy level for AMES security model is indicated in blue color and the energy level for other security model is indicated in orange color. The graph clearly shows that the least energy consumption is achieved by our AMES security model. The energy consumption of other security models is very high compared to our suggested model. The NS3 simulation is represented in fig. 6 where it shows the transmission of all the nodes, size of the node and the smooth factor. A clear snapshot is represented here along with the time factor represented in seconds. The simulation can be controlled with speed limit as well. We can able to see any selected node simulation or even for a disabled node.

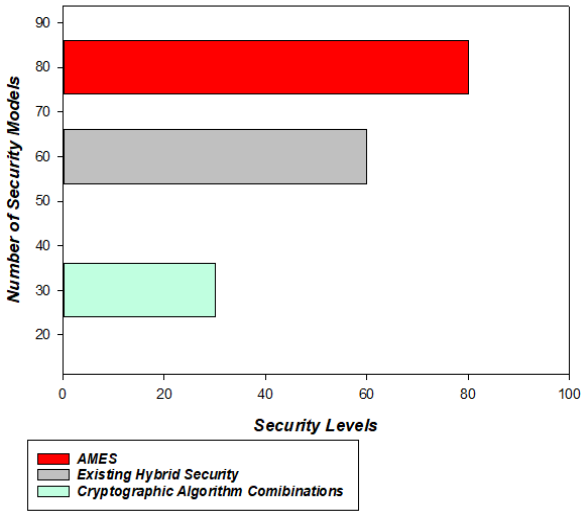


Fig. 4 – Security Level comparison graph

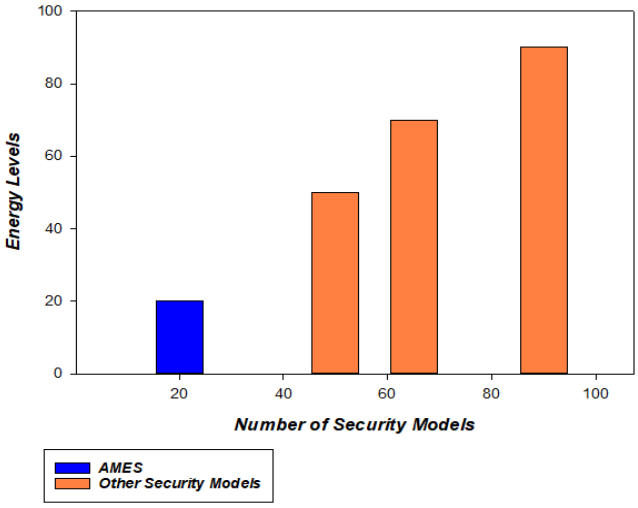


Fig. 5 – Energy Level Comparison of Security Models

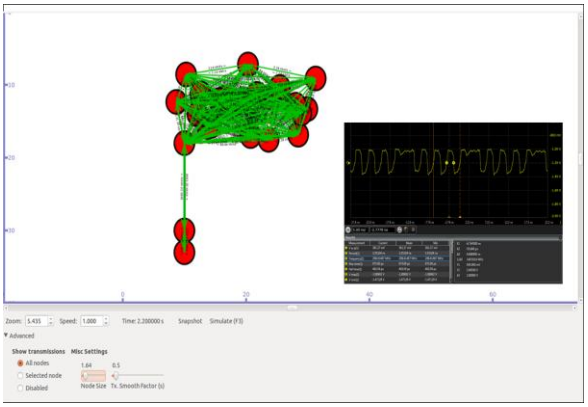


Fig. 6 – NS3 Simulation of Node Transmissions

In Fig. 7, a comparison is made between existing hybrid security model and the AMES security model based on the levels of attacks and the number of attacks. The device attacks are represented graphically by small dots and the communication attacks are graphically represented by black dots. The numbers of attacks are plotted from value '0' to '100'. The attack levels are plotted from value '0' to 100'. As seen from the graph, the number of attacks are more in the hybrid security system where as there are very less number of attacks in the AMES security system. From this we can conclude that the security level is very well achieved in our suggested AMES security model.

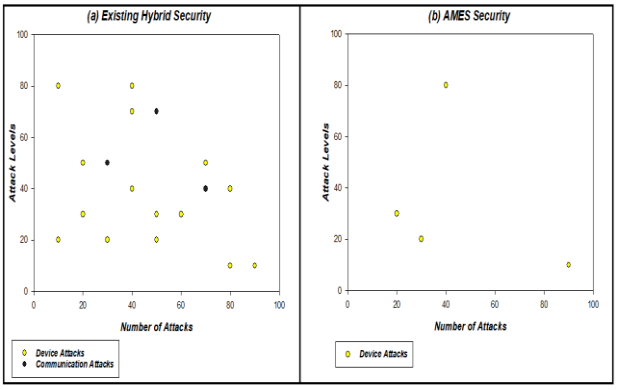


Fig. 7 – Number of Attacks comparison between AMES and Hybrid Security Models

V. CONCLUSION

IoT environment faces many security threats that need an immediate attention. With the help of our proposed AMES encryption model we can able to provide more security to the user credentials and to the network communication in the IoT environment. A protection to the user data is achieved with high level of encryption with the help of AMES encryption formula. We have used MQTT protocol instead of HTTP wince it is way faster to deliver all the packets without any damage. We have evaluated out suggested model with the help of NS3 simulation by comparing the factors – energy level, number of attackers, overall performance etc. In all these parameters AMES proved to be more effective and efficient in all means. Thus from our suggested method, all the security threats and difficulties faced in the IoT environment will be highly reduced with the help of AMES authentication system and MQTT protocol.

REFERENCES

1. Alcaraz, C. (2019). Security and Privacy Trends in the Industrial Internet of Things. Springer.
2. Zhang, J., Rajendran, S., Sun, Z., Woods, R., & Hanzo, L. (2019). Physical Layer Security for the Internet of Things: Authentication and Key Generation. IEEE Wireless Communications.
3. Jan, M. A., Khan, F., Alam, M., & Usman, M. (2019). A payload-based mutual authentication scheme for Internet of Things. Future Generation Computer Systems, 92, 1028-1039.
4. Rivera, D., García, A., Martín-Ruiz, M. L., Alarcos, B., Velasco, J. R., & Oliva, A. G. (2019). Secure Communications and Protected Data for a Internet of Things Smart Toy Platform. IEEE Internet of Things Journal, 6(2), 3785-3795.
5. Malik, M., Dutta, M., & Granjal, J. (2019). A Survey of Key Bootstrapping Protocols Based on Public Key Cryptography in the Internet of Things. IEEE Access, 7, 27443-27464.
6. Zeadally, S., Das, A. K., & Sklavos, N. (2019). Cryptographic Technologies and Protocol Standards for Internet of Things. Internet of Things, 100075.
7. Khattak, H. A., Shah, M. A., Khan, S., Ali, I., & Imran, M. (2019). Perception layer security in Internet of Things. Future Generation Computer Systems, 100, 144-164.
8. Khari, M., Garg, A. K., Gandomi, A. H., Gupta, R., Patan, R., & Balusamy, B. (2019). Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques. IEEE Transactions on Systems, Man, and Cybernetics: Systems.
9. Liu, J., Ren, A., Zhang, L., Sun, R., Du, X., & Guizani, M. (2019). A Novel Secure Authentication Scheme for Heterogeneous Internet of Thing. arXiv preprint arXiv:1902.03562.
10. Ferrag, M. A., Maglaras, L., & Janicke, H. (2019). Blockchain and its role in the internet of things. In Strategic Innovative Marketing and Tourism (pp. 1029-1038). Springer, Cham.
11. M. Sundarrajan, & A.E. Narayanan (2019). A Hardy Wall Encrypted System for Securing Iot Device Id International Journal of Recent Technology and Engineering (IJRTE), Vol 8, 586-590.
12. Elhoseny, M., Shankar, K., Lakshmanaprabu, S. K., Maseleno, A., & Arunkumar, N. (2018). Hybrid optimization with cryptography encryption for medical image security in Internet of Things. Neural computing and applications, 1-15.
13. Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 38, 8-27.
14. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities.
15. Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, 4(2), 118-137.
16. Cheng, C., Lu, R., Petzoldt, A., & Takagi, T. (2017). Securing the Internet of Things in a quantum world. IEEE Communications Magazine, 55(2), 116-120.

17. Trappe, W., Howard, R., & Moore, R. S. (2015). Low-energy security: Limits and opportunities in the internet of things. IEEE Security & Privacy, 13(1), 14-21.
18. He, D., & Zeadally, S. (2014). An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. IEEE internet of things journal, 2(1), 72-83.
19. Lee, J. Y., Lin, W. C., & Huang, Y. H. (2014, May). A lightweight authentication protocol for internet of things. In 2014 International Symposium on Next-Generation Electronics (ISNE) (pp. 1-2). IEEE.
20. Li, F., & Xiong, P. (2013). Practical secure communication for integrating wireless sensor networks into the internet of things. IEEE Sensors Journal, 13(10), 3677-3684.
21. Ning, H., Liu, H., & Yang, L. T. (2013). Cyberentity security in the internet of things. Computer, 46(4), 46-53.
22. Vučinić, M., Tourancheau, B., Rousseau, F., Duda, A., Damon, L., & Guizzetti, R. (2015). OSCAR: Object security architecture for the Internet of Things. Ad Hoc Networks, 32, 3-16.
23. Yaqoob, I., Ahmed, E., ur Rehman, M. H., Ahmed, A. I. A., Al-garadi, M. A., Imran, M., & Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. Computer Networks, 129, 444-458.
24. Sahraoui, S., & Bilami, A. (2015). Efficient HIP-based approach to ensure lightweight end-to-end security in the internet of things. Computer Networks, 91, 26-45.
25. Kim, H., Wasicek, A., Mehne, B., & Lee, E. A. (2016, August). A secure network architecture for the internet of things based on local authorization entities. In 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud) (pp. 114-122). IEEE.
26. Triantafyllou, A., Sarigiannidis, P., & Lagkas, T. D. (2018). Network protocols, schemes, and mechanisms for internet of things (iot): Features, open challenges, and trends. Wireless communications and mobile computing, 2018.
27. Hernandez-Ramos, J. L., Pawlowski, M. P., Jara, A. J., Skarmeta, A. F., & Ladid, L. (2015). Toward a lightweight authentication and authorization framework for smart objects. IEEE Journal on Selected Areas in Communications, 33(4), 690-702.
28. Chaimae, E., & Rahal, R. (2016, May). ECC certificate for authentication in cloud-based RFID. In 2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech) (pp. 200-203). IEEE.
29. Ning, H., Liu, H., & Yang, L. T. (2014). Aggregated-proof based hierarchical authentication scheme for the internet of things. IEEE Transactions on Parallel and Distributed Systems, 26(3), 657-667.
30. Liu, Z., Huang, X., Hu, Z., Khan, M. K., Seo, H., & Zhou, L. (2016). On emerging family of elliptic curves to secure internet of things: ECC comes of age. IEEE Transactions on Dependable and Secure Computing, 14(3), 237-248.
31. Kawamoto, Y., Nishiyama, H., Kato, N., Shimizu, Y., Takahara, A., & Jiang, T. (2015). Effectively collecting data for the location-based authentication in Internet of Things. IEEE Systems Journal, 11(3), 1403-1411.

AUTHORS PROFILE

M. Sundarrajan is currently pursuing his Ph.D. from Periyar Maniammai Institute of Science and Technology, Thanjavur, India. He had received his Master of Technology from SASTRA University, Thanjavur, India, and Bachelor of Engineering from PSV College of Engineering and Technology, Krishnagiri, India. He has good knowledge in the field of Internet of Things, Cyber-Physical System, Threat Intelligence and Data Security

A.E. Narayanan has Received his Ph.D. from Periyar Maniammai University, Thanjavur, India. He had received his Master degree from Manonmaniam Sundaranar University, Tirunelveli, India, and Bachelor of Engineering from Government College of Technology, Coimbatore, India. His current research interests include Wireless Sensor Networks, Smart Grid, Cryptography, Internet of Things and Threat Intelligence.