ISSN 1512-1232

ACHIEVING DATA AUTHENTICATION WITH HMAC-SHA256 ALGORITHM.

Nureni Ayofe Azeez[1] and Onyema Juliet Chinazo[2]

[1,2]Department of Computer Sciences, Faculty of Science,
University of Lagos, Lagos, Nigeria.
nazeez@unilag.edu.ng, chinazojinuka@yahoo.com

Abstract

Security and privacy of information being shared seamlessly in a distributed environment is very important. Failure to put in place, appropriate safety measure will give room for vulnerability. In order to ensure a secured information-sharing environment therefore, Keyed-Hash Message Authentication Code and Secured Hash Algorithm 256, HMAC-SHA256 was implemented. A Trust Based system that identifies the malicious nodes in the network and differentiates them from trusted nodes was also introduced. The trust value of the participating nodes is increased only for every successful transmission and decreased for those nodes that do not send the data towards the desired destination. The HMAC-SHA256 algorithm, which provided the desired results was implemented with Java programming language, HTML and CSS.

Keywords: *Network Security, Keyed_Hash_Message_Authentication_Code (HMAC), Malicious Nodes, Trusted Nodes; SHA-256*

INTRODUCTION

In recent times, information is fundamental for basic operations in every home, institution, organization and the society at large. Information involves computers, networks and communication media which are used to transmit the data from one point to another. Routing in a distributed network has become a big challenge to network security and there has been various studies and many researches in this field are attempting to propose more secure approach to it.

Verifying the integrity and authenticity of information is a prime necessity in computer networks as sensitive information are resident on computers and their networks. Message authentication is a process that allows communicating parties to verify that received messages are authentic. The two important aspects are verifying that the contents of the message have not been altered and that the source is authentic. Message Authentication Code (MAC) is a widely used technique for performing message authentication and this algorithm is not reversible unlike encryption/decryption algorithm.

In recent years, there has been increased interest in developing a MAC derived from a cryptographic hash code, such as MD5, SHA-1 and SHA-2. The security of any MAC function based on the embedded hash functions depends on the cryptographic strength of the underlying hash function. In this work, the cryptographic hash function used is SHA256- Secure Hash Algorithm, thus HMAC-SHA256 algorithm with a designed Trust Based System. This algorithm was evaluated to determine its effectiveness and efficiency.

ISSN 1512-1232

LITERATURE REVIEW

Wide Area Networks (WANs) are of great significance to network technologies (Vishal et. al., 2012). Many consequent security issues are associated with WANs, Bluetooth and cellular networks as they gained popularity in computer and business industry. Private and public environments enjoyed common access of WAN systems like IEEE 802.11 networks. Mobility and flexibility are some of the benefits of WAN (Guido, 2011). Compared to the traditional wired LAN, users enjoy more freedom for accessing the network, but such benefits also come with several security concerns.

Risks of wired networks and the new risks are all the security concerns in wireless environments posed as a result of mobility. To mitigate these risks and secure the users from eavesdropping, organizations have deployed several security mechanisms (Bulbul, Batmaz & Ozel, 2008). The basic WAN security mechanism is Wired Equivalent Protocol (WEP). WEP is an encryption algorithm that was designed in 1999 along with 802.11b standard to offer security wireless networks (Alexander & Albert, 2009). It employs RC4 (Rivest Cipher 4) algorithm from Rivest Shamir Adleman (RSA) data Security. In 2003, WEP was superseded due to the several serious weaknesses that were identified by cryptanalysts and that brought about the invent of Wi-Fi Protected Access (WPA) and then by the full IEEE 802.11i standard (also known as WPA2) in 2004.

In spite of the serious security flaws, WEP still offers a minimal level of security to networks. Institute for Electrical and Electronics Engineers (IEEE) 802.11 is a set of Wireless LAN standards developed by working group 11 of the IEEE 802 committee (Guido, 2011). The first 802.11 standard was released in October 1997 and revised in March 1999 as 802.1lb. The security mechanisms for secure communications on 802.11 wireless networks have been developed in the following chronological order (SANS,2010); Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and 802.11i (WPA2).

The use of the Advanced Encryption Standard (AES) is a more secure alternative to the RC4 stream cipher used by WEP and WPA (Tews & Beck, 2009). The WPA2 standard consists of two components, encryption and authentication which ensure security in WAN (Talegao, 2013). The encryption piece of WPA2 mandates the use of AES (Advanced Encryption Standard) but TKIP (Temporal Key Integrity Protocol) is available for backward compatibility with existing WAP hardware (Prasithsangaree & Krishnamurthy, 2003). WPA2 (along with WPA) resolved vulnerabilities of WEP to “hacker attacks such as ‘man-in-the-middle’, authentication forging, replay, key collision, weak keys, packet forging, and ‘brute–force/dictionary’ attacks” (Swati & Shilpi, 2012).

HMAC-SHA256 ALGORITHM

As encryption ensures only the confidentiality of the data being sent, a digital signature which is another security technique ensures other security goals like data authentication, non-repudiation and data integrity (Dilli & Chandra, 2014).

Hashing can be used in place of the digital process in long data or messages. In this, the data or message is passed through an algorithm called cryptographic hash function or one way-hash function (SHA256) before signing. Hashing creates a compressed image of the data in the form of a hash value or message digest which is usually unique and much smaller than the message. Any change made to the message produces a different hash result even if the same hash function is used.

Definition of HMAC-SHA256

HMAC-SHA256 defined as:

$$HMAC(K,m) = H((K \oplus opad) \parallel H((K \oplus ipad) \parallel m))$$

ISSN 1512-1232

which uses the following parameters:
H = cryptographic hash function = SHA256
K = secret key
m = message
‖ = concatenation
⊕ = exclusive OR
opad = outer padding
ipad = inner padding

The Trust Based System

The Trust Based System identifies malicious nodes in the network and differentiates them from the trusted nodes by providing a trust value to the participating nodes. For every successful data transmission, the trust value increases but decreases for nodes that do not send data to their destination or whose data has been altered or tampered with. This system in addition to the HMAC-SHA256 algorithm provides additional security to transmitted data. The trust based system gives a trust value of every node on the network. The trust value of a node or nodes increase if there is no attack on the sent data, this means the nodes are not malicious but decreases if malicious nodes exist.

EXPERIMENTAL RESULT AND ANALYSIS

As the program initializes, 'localhost: 8080/view' is typed in the web browser to bring up the front end of the application. Client and server nodes are created. In the client node, the column for the user-name, credentials, messages and the trust value are created while on server node, name and user's credentials are created.

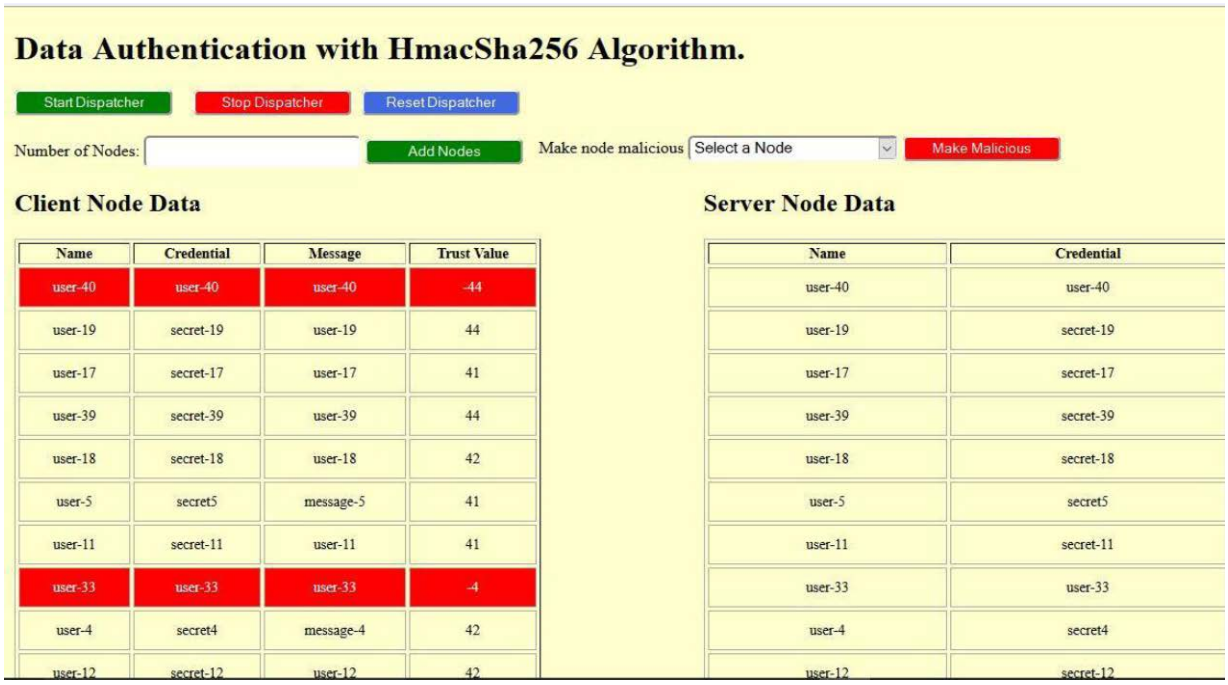
Once a user registers on the client node, the server node checks if the client's HMAC signature is the same as the registered HMAC signature on the server, if the two HMAC signature matches, then its packets are transmitted but if the client and the server's signature do not match, then the data or packets are considered malicious. And once a node is detected to be malicious, its trust value decreases to a negative but increases otherwise.

The study has shown that out of the one hundred nodes used, nodes: 19,10,32,33,40,41,43,45,47,49,82,83,84,85,94,95,97,98,86,87,88,89,90,91,92,93,96,99 and 100 act maliciously while nodes: 17, 18, 5, 11, 4, 12, 3, 20, 2, 9, 15, 1, 8, 16, 7, 13, 6, 14, 30, 31, 34, 35, 36, 37, 38, 39, 42, 44, 46, 48, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79 and 80 transferred data successfully and securely.

Two nodes- node 19 and node 10, are considered malicious while others are trusted nodes. The study of the second set of 10 nodes gives: Keyed-Hash Message Authentication Code with Secure Hash Algorithm 256, HMAC-SHA256, was successfully implemented in a distributed network with the Trust Based System differentiating the malicious and non-malicious nodes in the network by reducing the trust value of any tampered node on the network. With this, more secure data can be transmitted in the network thereby accomplishing the aim of data authentication and data integrity.

The extension of the authentication process used by WPA2 from just passphrase and encryption using the HMAC-SHA256 algorithm with Trust Based System was achieved. With the implementation of the above processes, data authenticity and data integrity are assured in a distributed system.

ISSN 1512-1232



Data Authentication with HmacSha256 Algorithm.

Start Dispatcher | Stop Dispatcher | Reset Dispatcher

Number of Nodes: | Add Nodes | Make node malicious | Select a Node | Make Malicious

Client Node Data

Name	Credential	Message	Trust Value
user-40	user-40	user-40	-44
user-19	secret-19	user-19	44
user-17	secret-17	user-17	41
user-39	secret-39	user-39	44
user-18	secret-18	user-18	42
user-5	secret5	message-5	41
user-11	secret-11	user-11	41
user-33	user-33	user-33	-4
user-4	secret4	message-4	42
user-12	secret-12	user-12	42

Server Node Data

Name	Credential
user-40	user-40
user-19	secret-19
user-17	secret-17
user-39	secret-39
user-18	secret-18
user-5	secret5
user-11	secret-11
user-33	user-33
user-4	secret4
user-12	secret-12

Figure 1. The second set of 10 nodes studied

As shown in Figure 1, Start Dispatch button, Stop Dispatcher button, Reset Dispatcher button, Add node button and Make Malicious button are used to give room for interactivity. Start Dispatch button is used to initiate sending of data packets from one node to the other. Reset Dispatcher button on the other hand terminates sending of the data packets in client's nodes. Reset Dispatcher button refreshes both the client and the server nodes while Add node button allows addition of desired number of nodes for the setup. Finally, Make Malicious button is used to make a node or more nodes to be malicious.

In the implementation, client and server nodes are also created. In the client node, the column for the user-name, credentials, messages and the trust value are created while on server node, name and user's credentials are created. Once a user registers on the client node, the server node checks if the client's HMAC signature is the same as the registered HMAC signature on the server, if the two HMAC signature matches, then its packets are transmitted but if the client and the server's signature do not match, then the data or packets are considered malicious. And once a node is detected to be malicious, its trust value decreases to a negative but increases otherwise.

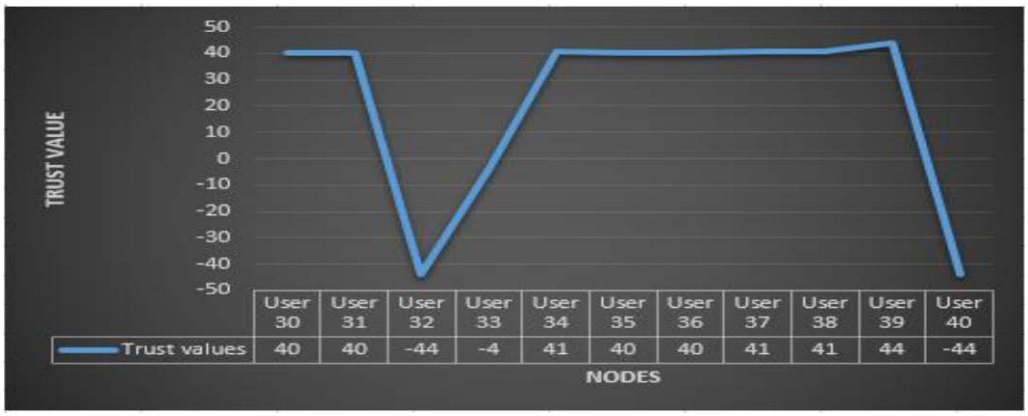


Figure 2. Graphical representation of the second set of 10 nodes

ISSN 1512-1232

It is shown from the graph that three nodes are malicious while others are not. This means that data sent to these malicious nodes have been tampered with or altered.

user-55	user-55	user-55	81	user-55	secret-55
user-12	secret-12	user-12	243	user-12	secret-12
user-56	secret-56	user-56	243	user-56	secret-56
user-53	secret-53	user-53	243	user-53	secret-53
user-10	secret-10	user-10	243	user-10	secret-10
user-54	secret-54	user-54	243	user-54	secret-54
user-15	secret-15	user-15	243	user-15	secret-15
user-59	secret-59	user-59	242	user-59	secret-59
user-16	secret-16	user-16	242	user-16	secret-16
user-13	secret-13	user-13	241	user-13	secret-13
user-57	secret-57	user-57	242	user-57	secret-57
user-14	secret-14	user-14	241	user-14	secret-14
user-58	secret-58	user-58	241	user-58	secret-58
user-51	secret-51	user-51	241	user-51	secret-51
user-52	secret-52	user-52	241	user-52	secret-52

Figure 3. Output representation of nodes 40-50

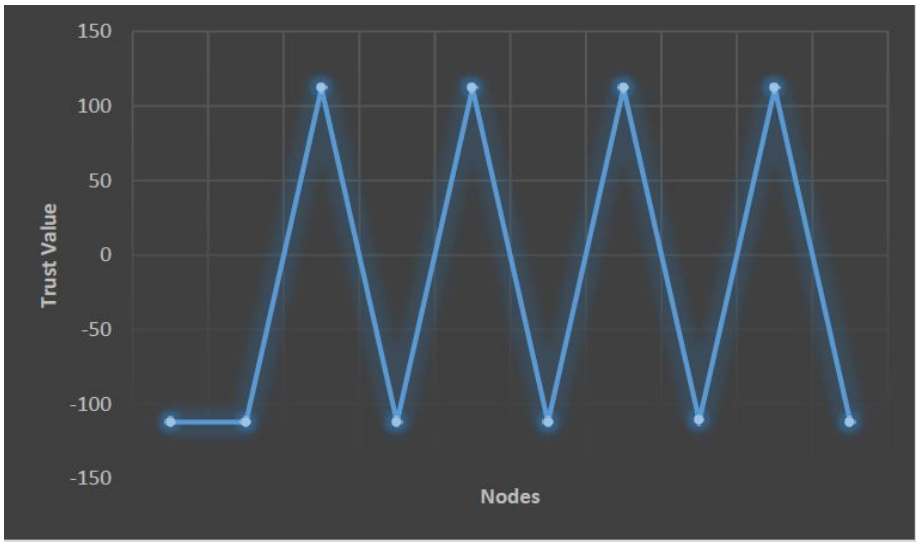


Figure 4. Graphical representation of nodes 40-50

In the graphical representation of nodes ranging from 40 to 50 of Figure 4, six nodes are seen to be malicious while four node are not.

ISSN 1512-1232

Table 1. Tabular representation of nodes 51-61

Nodes	Trust value
User 51	241
User52	244
User53	243
User54	243
User55	81
User56	243
User57	242
User58	241
User59	242
User60	244

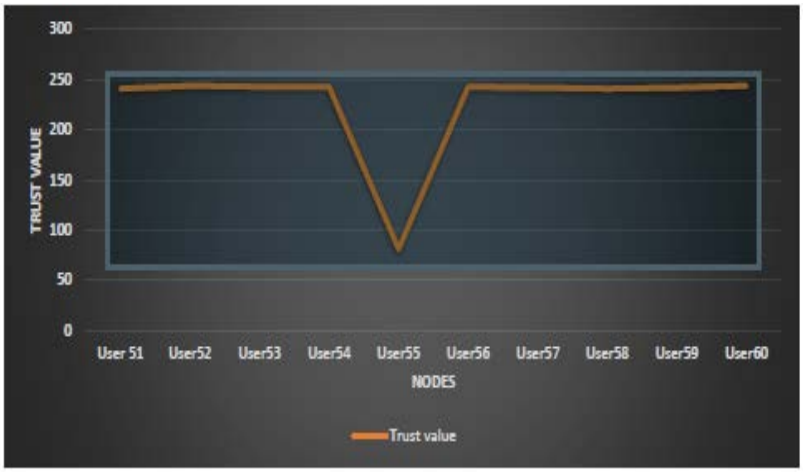


Figure 5. Graphical representation of users ranging from 51 to 60.

From Figure 5, only one node - User 55, is seen to be insecured while others are secured.

Client Node Data

Name	Credential	Message	Trust Value
user-80	user-80	user-80	-825
user-81	user-81	user-81	-587
user-40	secret-40	user-40	823
user-41	secret-41	user-41	825
user-39	secret-39	user-39	823
user-5	secret5	message-5	823
user-33	secret-33	user-33	823
user-77	secret-77	user-77	825
user-4	secret4	message-4	825
user-34	secret-34	user-34	823
user-78	secret-78	user-78	823
user-3	secret3	message-3	823
user-31	secret-31	user-31	823
user-75	secret-75	user-75	823

Server Node Data

Name	Credential
user-80	secret-80
user-81	secret-81
user-40	secret-40
user-41	secret-41
user-39	secret-39
user-5	secret5
user-33	secret-33
user-77	secret-77
user-4	secret4
user-34	secret-34
user-78	secret-78
user-3	secret3
user-31	secret-31
user-75	secret-75

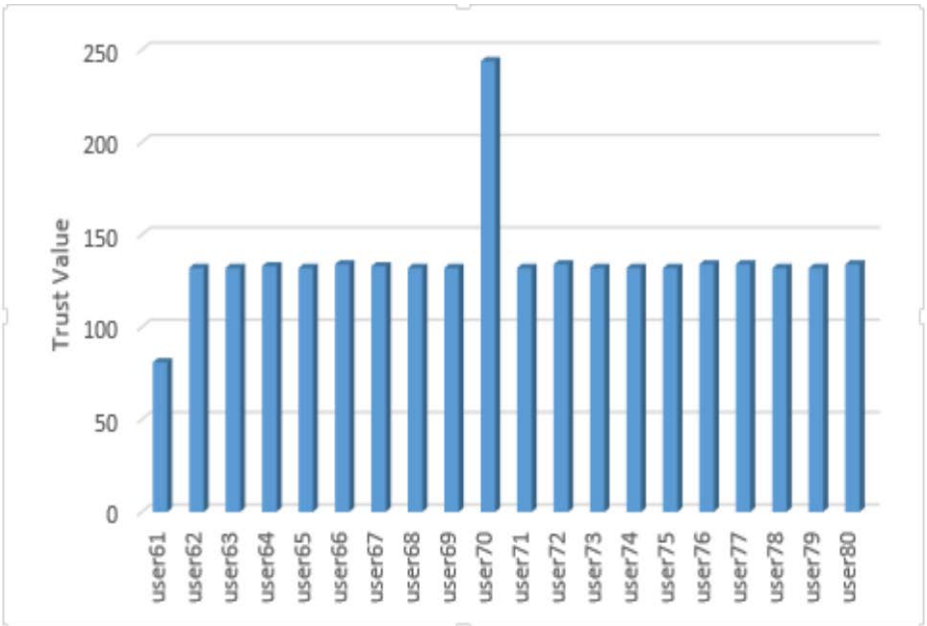
ISSN 1512-1232

Figure 6. Trust values of nodes ranging from 61 to 81

In the output representation of nodes 61 to 81, there has been successful transmission of data up to user 53 but user 80 gave an error message implying that the user client's HMAC signature and its server HMAC signature do not match. The output is tabulated in Table 2 and its corresponding graphical representation is provided in Figure 7.

Table 2: Trust value of nodes 61 to 81

Nodes	Trust value
user61	81
user62	132
user63	132
user64	133
user65	132
user66	134
user67	133
user68	132
user69	132
user70	244
user71	132
user72	134
user73	132
user74	132
user75	132
user76	134
user77	134
user78	132
user79	132
user80	134



ISSN 1512-1232

Figure 7. Graphical representation of nodes ranging from 61 to 81

Table 3. The tabular representation of the last set of nodes

Nodes	Trust value
user82	-249
user83	-244
user84	-244
user85	-252
user86	132
user87	576
user88	133
user89	132
user90	166
user91	244
user92	132
user93	134
user94	-113
user95	-209
user96	132
user97	-166
user98	-136
user99	132
user100	132

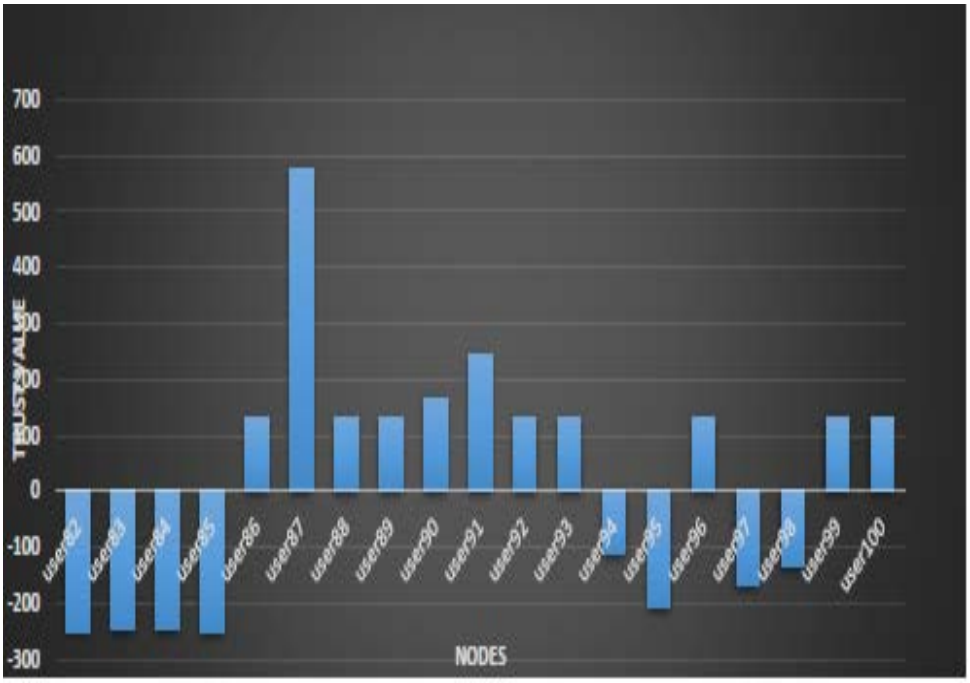


Figure 8. Graphical representation of nodes ranging from 81 to 100

CONCLUSION

From the above study, nodes 19, 10, 32, 33, 40, 41, 43, 45, 47, 49, 82, 83, 84, 85, 94, 95, 97, 98, 86, 87, 88, 89, 90, 91, 92, 93, 96, 99 and 100 acts maliciously based on various characteristics exhibited at the implementation stage while nodes 17, 18, 5, 11, 4, 12, 3, 20, 2, 9, 15, 1, 8, 16, 7, 13 ,6, 14, 30, 31, 34, 35, 36, 37, 38, 39, 42, 44, 46, 48, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79 and 80 are the trusted nodes.

This implies that HMAC-SHA256 Algorithm with Trust Based System as proposed and demonstrated is capable of enhancing data authentication and data integrity. This was achieved by detecting the untrusted nodes and separating them completely from the trusted ones.

REFERENCES

1. Alexander, G & Albert, L 2009, 'Wired Equivalent Privacy (WEP) Functionality, Weak Points and Attacks', University, Freiburg, vol. 2, no.3, pp 4-7.
2. Arana, P 2006, 'Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2)', INFS 612-Fall, vol.3, no. 4, pp 6-8.
3. Atasu K, Breveglieri, I, Macchetti, M 2004, 'Efficient AES Implementations For ARM Based Platforms,, Proceedings of the 2004 ACM symposium on Applied computing, vol. 3, no. 2, pp 4-6.
4. Bernard, A, Larry, J, Blunk, J, Vollbrecht, R, James, C, & Henrik, L, 2004, 'Extensible Authentication Protocol (EAP)', Internet RFC 3748, pp 14-16.
5. Doomun, M. R & Soyjaudah, K. M. 2007, 'Adaptive IEEE 802.11i security for energy security optimization', The Third Advanced International Conference on Telecommunications, 2007. AICT vol. 3, no. 5, pp 1-13.

ISSN 1512-1232

6. Dworkin, M 2004, 'Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality', NIST Special Publication 800- 38C, pp 5-8.
7. Edney J. & Arbaugh W. A. 2003, 'Real 802.11 Security: WiFi- Protected Access and 802.11i', Addison Wesley, New York, NY, USA, vol. 5, no. 3, pp. 12-14.
8. Edney & William, A. 2003, 'Real 802.11 Security: Wi-Fi Protected Access and 802.11i', Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, vol. 6, no. 5, pp 7-9.
9. Frank, H & Katz, 2010, 'WPA vs. WPA2: Is WPA2 Really an Improvement on WPA?', 4th Annual Computer Security Conference (CSC 2010), Coastal Carolina University, Myrtle Beach, SC. vol. 4, no. 5, pp 9-15.
10. Furnell, S & Warren, M 1999), 'Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?' Computers and Security, vol. 18, no. 12, pp. 28-34.
11. Joan, D & Vincent, R 2002, 'The Design of Rijndael: AES -The Advanced Encryption Standard (Information Security and Cryptography)', 2nd edn, Springer, USA, pp 76-38.
12. Joon, S. P & Derrick, D 2003, 'WLAN Security: Current and Future', IEEE Computer Society, Syracuse University, NY, USA. Pp 12-14. Labib, K 2004, 'Computer Security and Intrusion Detection', Crossroads, vol. 11, no. 1 pp. 2-4.
13. Lehembre, G 2005, 'Wi-Fi Security -WEP, WPA and WPA2', Hakin9.org Newsletter, pp 1-3.
14. Matthieu, C & Jean-Loup 2010, 'Attacks against the WiFi protocols WEP and WPA', vol. 3, no. 4, pp 7-9.
15. Mirkovic & Reiher, P 2004, 'A Taxonomy of DDoS Attack and DDoS Defense Mechanisms', Computer Communication Review, vol. 34, mo. 2, pp. 39-53.
16. Mohammed, F & Shawkat, A 2015, 'Recurrent security gaps in 802.11ac routers', International journal of scientific & technology research vol. 4, no. 9, pp 12-14.
17. Naamany, Al, Ahmed, M, Shidhani, A & Bourdoucen, H 2006, 'IEEE 802.11 wireless LAN security overview', IJCSNS, vol. 6, no. 7, p. 138.
18. Nazmus, AKM, Sakib, F, Tasmin, J, Muntasim, M &Armin, A2011, 'Security Improvement of WPA 2 (Wi-Fi Protected Access 2)', International Journal of Engineering Science and Technology (IJEST), vol. 3 No. 1, pp 7-9.
19. Newman, R 2006, 'Cybercrime, Identity Theft and Fraud: Practicing Safe Internet – Network Security Threats and Vulnerabilities', Proceedings of the 3rd Annual Conference on Information Security Curriculum Development. New York, USA, vol. 6, no. 3, pp. 68-78.
20. Nidal, T & Florica, M 2009, 'A Comparison between Wireless LAN Security Protocols', Series C, ISSN: 1454-234x, Scientific Bulletin of UPB, vol. 71, no. 1, pp 43-46.
21. Park, JS & Dicoi, D 2003, 'WLAN security: current and future', IEEE Internet Computing, vol. 7, no. 5, pp. 60–65.
22. Pash, A 2012, 'How to crack a Wi-Fi Network's WPA Password with Reaver in LifeHacker', p 21-16.
23. Rango, F.D, Lentini, D.C & Marano, S 2006, 'Static and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack in Wi-Fi Protected Access and IEEE 802.11 I. EURASIP', Journal on Wireless Communications and Networking, pp. 73-93.
24. Roche, W 2006, 'The Advanced Encryption Standard, The Process, Its Strengths and Weaknesses', University of Colorado, Denver, Spring 2006 Computer Security Class, CSC 7002, Final Paper, pp 4-9. 48.
25. Ayofe, A.N, Adebayo, S.B, Ajetola, A.R, Abdulwahab, A.F (2010) "A framework forcomputer aided investigation of ATM fraud in Nigeria" International Journal of Soft Computing, Vol. 5, Issue 3 pp. 78-82
26. Azeez, N.A, Olayinka, A.F, Fasina, E.P, Venter, I.M. (2015) "Evaluation of a flexible column-based access control security model for medical-based information" Journal of Computer Science and Its Application. Vol. 22, Issue 1, Pages 14-25.
27. Azeez, N. A., and Ademolu, O. (2016). CyberProtector: Identifying Compromised URLs in Electronic Mails with Bayesian Classification. 2016 International Conference Computational Science and Computational Intelligence (CSCI) (pp. 959-965). Las Vegas, NV, USA: IEEE.

ISSN 1512-1232

28. Azeez, N. A., and Babatope, A. B. (2016). AANtID: an alternative approach to network intrusion detection. The Journal of Computer Science and its Applications. An International Journal of the Nigeria Computer Society, 129-143.
29. Azeez, N. A., and Iliyas, H. D. (2016). Implementation of a 4-tier cloud-based architecture for collaborative health care delivery. Nigerian Journal of Technological Development, 13 (1), 17-25.
30. Azeez, N. A., and Venter, I. M. (2013). Towards ensuring scalability, interoperability and efficient access control in a multi-domain grid-based environment. SAIEE Africa Research Journal, 104 (2), 54-68.
31. Azeez, N. A., Iyamu, T., and Venter, I. M. (2011). Grid security loopholes with proposed countermeasures. In E. Gelenbe, R. Lent, and G. Sakellari (Ed.), 26th International Symposium on Computer and Information Sciences (pp. 411-418). London: Springer.
32. Azeez, N.A., and Lasisi, A. A. (2016). Empirical and Statistical Evaluation of the Effectiveness of Four Lossless Data Compression Algorithms. Nigerian Journal of Technological Development, Vol. 13, NO. 2, December 2016, 64-73.
33. Nureni, A. A., and Irwin, B. (2010). Cyber security: Challenges and the way forward. Computer Science & Telecommunications, 29, 56-69.
34. Azeez, N.A and Venter, I.M (2012). Towards achieving scalability and interoperability in a triple-domain grid-based environment (3DGBE)- Information Security for South Africa (ISSA), 2012, pp 1-10.
35. Azeez N.A and Otudor A.E (2016) "Modelling and Simulating Access Control in Wireless Ad-Hoc Networks" Fountain Journal of Natural and Applied Sciences. Vol 5(2), pp 18-30.
36. Azeez, N.A Abidoye, A.P Adesina, A.O Agbele, K.K Venter, I.M Oyewole, A.S(2013) "Statistical Interpretations of the Turnaround Time Values for a scalable 3-tier grid-based Computing architecture" Computer Science & Telecommunications, Vol 39 (3), pp 67-75.

Article received: 2018-03-30