ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2021.0349

BIO-INSPIRED BASED SEGMENTATION AND USER AUTHENTICATED KEY MANAGEMENT FOR IOT NETWORKS

M. Savitha[1] and M. Senthilkumar[2]
[1]*Department of Computer Science, Government Arts College, Udumalpet, India*
[2]*Department of Computer Science, Government Arts and Science College, Avinashi, India*

Abstract

Data exchanging and gathering is greatly achieved by several interconnected physical objects or smart devices over the Internet are termed as Internet of Things (IoT). A generic IoT network called Hierarchical IoT Network (HIoTN) inclusive of the organized different nodes in a hierarchy as gateway node, cluster head nodes and sensing nodes. In HIoTN of generic IoT networking environment for a particular application, user direct access in real-time data from the sensing nodes is necessitated. Recent work introduces a User Authenticated Biometric Key Management Protocol (UABKMP) for IoT network. Hence this proposed work exhibits new region of interest based segmentation algorithm with base procedure of Modified Bat optimization (MBO) algorithm hybrid with Active Contour Model. In the MBO algorithm the parameters of the bat is tuned via the use of the Brownian Distribution. Finally an Authenticated Key Management (AKM) is proposed for IoT network. The Real-Or-Random (ROR) model is incorporated in network for proving the scheme formal security and also ensures the informal security being protected from several probable attacks.

Keywords:

Hierarchical IoT Network, Authentication, Key Management, Security, Segmentation, Modified Bat Optimization, Active Contour Model, Iris

1. INTRODUCTION

The Internet of Things (IoT) is made up of several connected devices that form a large network that connects smart devices such as sensors, actuators, and so on, and these devices are mostly used in various sectors such as public health, smart grids, smart transportation, waste management, smart homes, smart cities, agriculture, energy management, and so on. A number of challenges are seen with the demands and constraints of the linked stuff pose, including interconnected multi-machines for interacting with each other, and ensures the necessity of safeguarding IoT networks from being attacked (in the last three years, according to Gartner study, 20% of organizations have come across at least one IoT attack [1]) and becoming an attack tool at the same time. Conventional communication protocols and security schemes are considered inefficient and infeasible for IoT devices with a resource-limited nature. Because of their pervasiveness and implementation, IoT safety issues in critical apps are being approached with caution, as any safety violation can be life-threatening. In IoT authentication schemes, the heterogeneity of devices in IoT networks is focused mainly on high security and further functionality features. HIoTNs are primarily required to support existing authentication protocols. A generic IoT network known as the Hierarchical IoT Network (HIoTN) is made up of different nodes organized in a hierarchy such as gateway nodes, cluster head nodes, and sensing nodes.

The IoT network is required based on its application sort, security needs, confidentiality, integrity and/or authentication [5]. The network efficiency is determined by the devices that are interconnected in an IoT network. A single compromised node can wreak havoc on the network by being malicious or causing disasters [6].Unlike other research works, [7] presented an interactive key management protocol besides a non-interactive key management protocol for mitigating communication cost of things.

The proposed schemes are resilient to several attacks and as wireless sensor networks built by resource-limited IoT devices: Zolertia Zoul remote exhibited security analysis by [8] proposing a lightweight PUF-based authentication protocol. The DTLS protocol, as a user datagram protocol (UDP), provides unreliable transport while using fewer resources [9]. Another cloud-based [10] application is smart home, which is based on IoT architecture and uses an IoT smart Hub (ISH) to communicate with home appliances and smart devices. The command sent from the cloud-connected smart phone to the IoT smart Hub (ISH) via the internet may result in an external attack. An application with a five-staged automated security framework protects against potential attacks, security investigations, and various defense strategies performance evaluation.

In [12], an outline of authentication protocols for IoT is chosen and investigated. In [13], an IoT device provides physically unclonable functions and wireless signal characteristics by means of a two-factor authentication. In [14], physical attack is prohibited by two-factor authentication techniques including PUFs. In [15], a multi-key (or multi-password) based mutual authentication mechanism is presented for secure vault meant for secret sharing among IoT servers and devices with equal sized keys.

In [16], an authentication protocol based on a distributed cloud environment and smartcards is used to secure the information of registered users across all private cloud servers. The identity issues of the identity management framework are given an overview. The identity issues of the identity management framework are given an overview. In [17], two novel lightweight CRL protocols with tailored on constrained IoT end-devices are developed for maximum flexibility. In [18], the AKM mechanism includes the resource constraints of IoT devices without pre-configured security information amid access network domain and IoT service domain to delegate AKM processes burden to a powerful agent. On IoT security [19], authentication is used to implement a mechanism based on X.509 digital certificates that has a significant effect.

Based on a Cloud-IoT network, [20] presented an efficient, strong authentication protocol for MP in healthcare applications to access patient data. In [21], a multi-criteria classification is provided by comparison and analysis of the different authentication schemes but faced with many pros and cons. A user-authenticated key management protocol [22] was developed

for simple sensing devices with limited security aspects, but it is not practical for complex IoT architectures. However, the more security is motivated by biometric results, the better. Then, in the proposed work, segmentation methods are introduced to segment the exact area of the individual user, which increases the further security of human participation, as well as accuracy and efficiency enhancements, resulting in cost-effective profit. The key contribution is as follows:

- Initially, User Authenticated Biometric Key Management Protocol (UABKMP) is developed for remote user authentication with iris biometric in HIoTN deployment.
- Use of cryptographic hash function incorporating symmetric encryption/decryption gives efficient result. Biometrics based authentication is best against traditional methods of authentication. Biometric based authentication usage to access our personal devices is more convenient.
- In this biometric, the segmentation is done using hybrid MBO, this method is implemented to select the Region of Interest of iris biometric images that is used for user authentication.
- The ROR model is integrated for scheme formal security. Additionally, ensures the informal security being protected from several probable network attacks.
- To ensure security, the AVISPA tool performs scheme formal security verification via simulation. The system architecture is given in Fig.1.

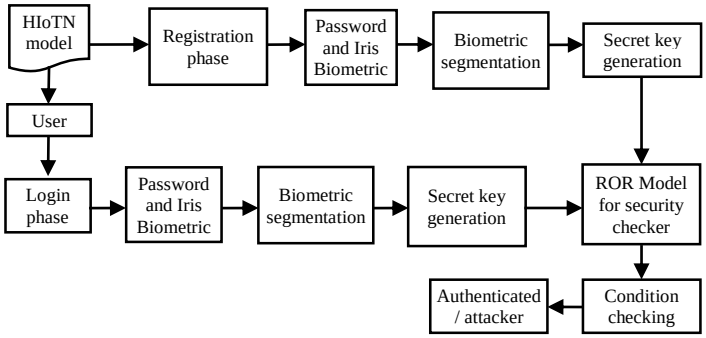

Fig.1. Proposed UAKMP for IoT Architecture Diagram

This proposed work is organised as follows: The network model incorporating threat model associated with UAKMP the various phases related to UAKMP, security analysis with hybrid MBO segmentation is presented in Section 2. Section 3 explicates the experimental outcomes and discussion and final segment exhibits conclusion and potential work in future.

2. SYSTEM MODEL

A hierarchical IoT-based smart home architecture is revealed in Fig.2 in which there are two groups namely appliance group and monitor group acts as agents installed in this smart device. The communication with central controller through wireless medium is accomplished through agents and user interface helps user controlling the smart home system. Also, any smart device information can be accessed by user by central controller. But, various threats are associated with HIoTNs [23] [24], and therefore, security is regarded as an essential prerequisite for protecting against various attacks. The smart devices connection is done to Internet via their nearby gateway node (GWN) in all these situations. Consequently, a secure user authentication protocol for HIoTNs is greatly necessitated for accessing real-time sensitive information from the sensing nodes in the HIoTN by an authorized external party (user). There arises numerous threats due to sensing nodes deployment in a hostile environment, which wireless communication is considered to be not secured. In addition, there are various security restrictions for most of the prevailing authentication protocols, such as impersonation, sensing node capture, man-in-the-middle, replay and privileged insider attacks. This provides a motivation for designing a more secure and reliable user authentication scheme for HIoTN.

2.1 NETWORK MODEL

The network model for specific HIoTN in UAKMP is designed [25] are shown in Fig.2. Various hierarchical structures are motivated based on IoT applications. In every HIoTN application with one gateway node (GWN), the resource-constrained sensing nodes (SN_k) in network model and cluster head nodes (CH_j) present in resource and most powerful gateway node (GWN) are present with structure of hierarchy. Quite a lot of sensing nodes are installed depending on IoT applications like disjoint clusters as shown in Fig.2. CH forwards information to GWN that received from a sensing node SN_k of individual cluster of sensed information from own CH_j. It is to be noticed of communication among sensing nodes besides corresponding cluster heads (CHs), and via the wireless channels the CHs and the GWN are performed.

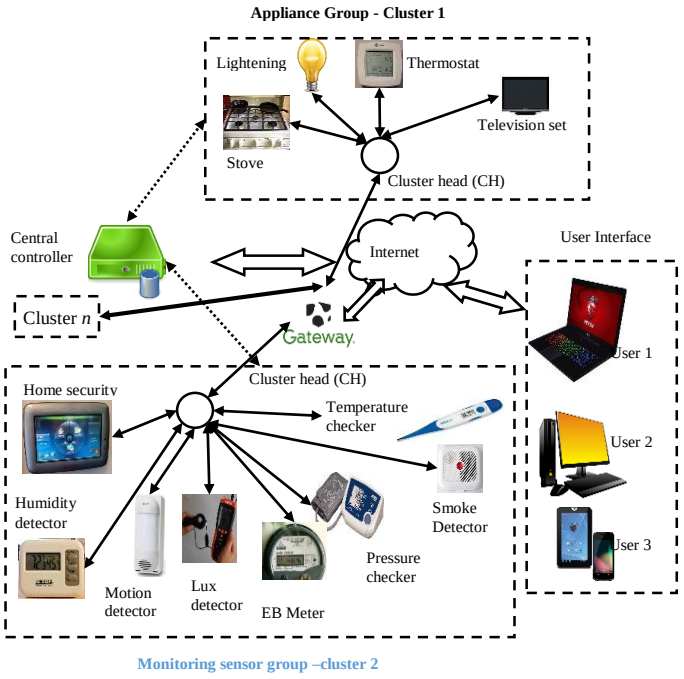

Fig.2. A hierarchical IoT-based smart home architecture

2.1.1 User Authenticated Key Management Protocol For HIoTN:

The six phases of UAKMP are as follows as and elucidated:

Step 1: Registration of sensing node in offline

Step 2: Every user registration

Step 3: Every user login are encountered

Step 4: Perform Authentication and analyse key agreement

Step 5: Updation of biometric password

Step 6: Deployment of new sensing node.

Registration of Sensing Node in Offline Phase: Gateway node (GWN) registers and executes the offline sensing. Initially at registration time, password is chosen as 160-bit long random secret key K on every installed sensing node SN_k, and the temporal credential of SN_k as TC_{SN_k} is determined. Consequently, the information $\{TC_{SN_k}, ID_{SN_k}\}$ are stored into the memory of SN_k before HIoTN, where ID_{SN_k} is SN_k's identity and TC_{SN_k} is the temporal credential.

User Registration Phase: Real-time information is utilized from sensing nodes SN_k and user U_i registration process is necessitated at GWN. This phase needs the subsequent steps:

Step 1: *Password*: U_i picks a password PW_i on user choice then a 128-bit random secret r_a, computes masked password == $h(PW_i||r_a)$. The registration request $\langle MPW_i \rangle$ is passed to the GWN by U_i.

Step 2: *Biometric*: Following in receipt of PW_i imprints his/her personal biometrics (iris) BIO_i, once U_i at a particular terminal sensor the segmentation of biometric images is done using Modified Bat Algorithm (explained below) and the resultant segmented biometrics $SBIO_i$ is utilized in this work to generate the key, PW_i is ready for computing secret biometric key σ_i and public parameter τ_i by fuzzy extractor probabilistic generation function as $Gen(SBIO_i) = (\sigma_i,\tau_i)$ [26]. At the end, the information $\{BIO_i, MPW_i, \tau_i, Gen(\cdot), Rep(\cdot), t\}$ are loaded in SC_i, where error tolerance parameter applied in $Rep(\cdot)$ is t.

2.2 IRIS SEGMENTATION USING HYBRID MBO FOR GENERATING SEGMENTED BIOMETRICS

Some of techniques as global thresholding, watershed segmentation, clustering techniques, region-growing and active contour model are put in practice for image segmentation method [27]. A snake model is also considered under the impact of an inner and external force for contour energy optimization. The primary problems in the snake model are the iterative of contour initialization, on the local minima its contour convergence in encroachment, and the manual choice of internal energy parameters weight. This results in the incorrect delineation of the region of concern resulting in the iris picture being incorrectly segmented. In this part, MBA executes the active contour model's (ACM) problems and to produce the precise segmentation of the biometric image input iris that is checked by the user's authentication process. MBO algorithm along ACM practical adapt external energy weights and elopes local minima through classical snake method. In UABKMP, similarity measures amid MBO-ACM algorithm and expert segmented image $SBIO_i$ attains high as user registration phase input. The Fig.3 expose the proposed MBO-ACM.

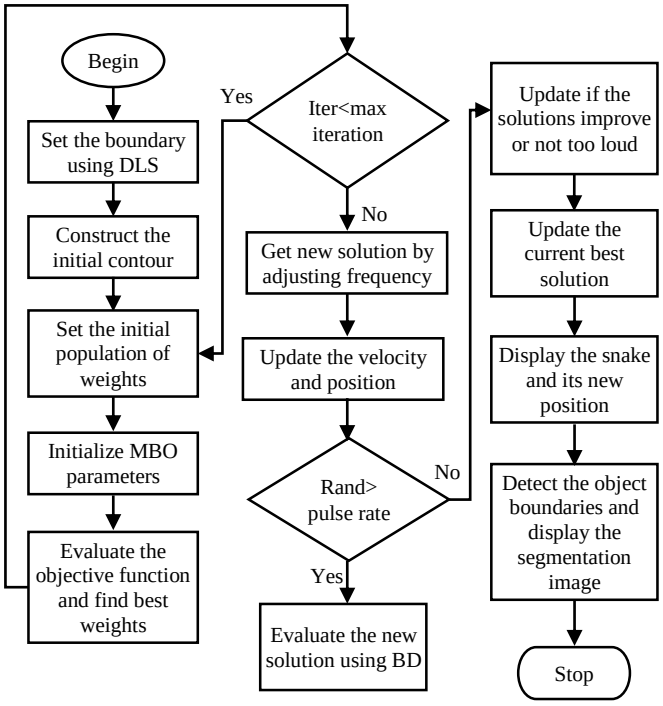

Fig.3. Flowchart of proposed Hybrid MBO-ACM

Active Contour Method: The pupil noncircular shape and the iris makes difficult in segmentation of the iris image when shape varies based on image acquisition methods. The two steps are followed in the iris segmentation as for approximate iris inner (pupil) and outer (iris) boundaries by elliptical model and Direct Least Square (DLS) determines the exact iris inner and outer boundaries on the basis of approximated boundaries by applying the region-based active contour model. Minimal boundary skin regions are taken including pupil and iris regions possible. The segmentation process is explained with base fact of active contour approach or snakes i.e., deformable splines under internal and external forces effect. The contour smoothness are controlled by internal force and pulls contour towards object boundaries are pulled out by the external force based on image features such as line and image gradient [12]. The minimization of the total energy E_T determines the deformation of the contour as:

$$E_T = E_{inl}(C) + E_{exl}(C) \quad (1)$$

The contour is denoted by C, contour internal energy as $E_{inl}(C)$ is and contour external energy $E_{exl}(C)$. The $E_{inl}(C)$ is expressed in terms of first and second derivatives of the contour and is given as [13]:

$$E_{exl}(C) = w_1(C)\left|\frac{dC(cp)^2}{dcp}\right| + w_2(C)\left|\frac{d^2C(cp)^2}{d^2cp}\right| \quad (2)$$

where, w_1 and w_2 denotes weights to the energy terms and cp denotes contour control point .

At the same point, $E_{exl}(C)$ is calculated as follows:

$$E_{\text{exl}}(C)=w_lE_l+w_\varepsilon E_\varepsilon+w_tE_t \quad (3)$$

where w_l, w_E and w_t are the line weight, edge weight and term weights of the energy term. In this event, curve is evolved from inside approximated iris boundary for reducing eyelids and eyelashes effects. The ACM implementation is carried out by subsequent steps:

Step 1: Input iris image and preprocessing of image

Step 2: Insight discrete points and also establish the contour via the sample points on curve

Step 3: Initialize parameter readings for snake evaluation

Step 4: Establishing pentagonal matrix where w_1, w_2 is the coefficient values and condition verify, Iterations = Maximum Iterations

Step 5: Foreshadowing and establishing spline to final contour.

Step 6: Final segmentation result

MBO: The traditional BAT (BAT) has three mathematical discrete equations, defining velocity update, position update, and frequency vector as specified below:

$$V_i(t+1) = V_i(t)+(X_i(t)-G_{best})F_i \quad (4)$$

$$X_i(t+1) = X_i(t)+V_i(t+1) \quad (5)$$

$$F_i=F_{min}+(F_{max}-F_{min})\beta \quad (6)$$

where β represents random integer in the range [0,1]. From $V_i(t+1)$, it is noted that, velocity update chiefly relies on frequency vector. In the course of optimization search, a new solution generation for each bat is done based on the succeeding relation: $X_{new}=X_{old}+\varepsilon A^t$ where ε represents random numeral in the range [-1,1] and annotates emitted sound loudness by bats throughout search space exploration.

The minimum value of 0 loudness variable A is selected as A_0 = 10, and A_{min} = 1, which decay in steps of 0.01. Other related mathematical representations for loudness adjustment are offered below:

$$A_i(t+1) = \alpha A_i(t),\ r_i(t+1) = r_i(0)[1-\exp(\gamma t)] \quad (7)$$

where α and γ denotes constants typically assigned with a numeral value of 0.75. In [28] reported that, TBA performance can be enhanced through Lévy Flight (LF) scheme. The random numerical value 'ε' in the new bat position X_{new} is substituted with a Lévy operator. In the anticipated work, 'ε' is substituted with a Brownian Distribution (BD) parameter recently discussed [28] and LF and BD combined in the proposed BAT the algorithm is named as MBO, where Bat new position can be stated with the succeeding relation:

$$X_{new} = X_{old}+A^t \oplus LF \quad (8)$$

$$X_{new} = X_{old}+A_t \oplus BD \quad (9)$$

The above equation represents the position expression for LF and BD based BAT. The BD is a subdiffusive non-Markovian process, which follows a Gaussian distribution with zero mean and time dependent variance [28].

2.2.1 Login Phase:

Login phase is ready once the completion of registration process of a user U_i as of following steps:

Step 1: Completing the identity process, each user enters the biometric information ($SBIO_i'$) and password at the sensor of the card reader, GWN make progress to improve secret biometric key as $\sigma_i' = Rep(SBIO_i', \tau_i)$ performing that the Hamming distance between $D(SBIO_i, SBIO_i')$ at registration time for equivalent or less than threshold value t.

Step 2: GWN then calculates r_a*as in [25] and checks whether D_i*= $D_i.U_i$ is said to be valid on satisfying condition U_i else do iteration.

Step 3: After selecting one time secret x_1 and current time stamp T_1, U_i enters the identity of an accessed sensing node N_k, and compute

$$M_1 = E_{TC_{U_i^*}}\left(x_1, ID_{SN_k}\right) \quad (10)$$

$$M_2 = h\left(x_1 \| PW_i \| ID_{GWN} \| ID_{SN_k} \| T_1\right). \quad (11)$$

Finally the login request message will be $\langle PW_i^{**}, M_1, M_2, T_1\rangle$ is then transmitted publically.

2.2.2 Authentication and Key Agreement Phase with ROR Model:

Once in receipt of the login request message from section 2.1.3 the following steps are taken place to execute the authentication and session key SK establishment between (U_i,SN_k) through GWN.

Step 1: Checking the condition that $|T_1-T_1^*| \leq \Delta T_1$, where ΔT_1 is the maximum transmission delay. After that the decryption of M_1 is done using temporal credential TC_{Ui} and stored in a database.

Step 2: The GWN is computes M_3 as in [26] and checks M_3= M_2. If condition is met the new $TempID_{SNk}$ is generated else the session stops instantly and calculates M_4 and transmits via CH_j

Step 3: After receiving M_4 at time T_2* and check $|T_2- T_2^*| \leq \Delta T_2$, where Δ T_1 notates maximum transmission delay, if condition is met the M_4 will be decrypted and checks M_3=M_2. Else the connection ceases instantly and choosing one time secret x_2 and current timestamp T_3, compute M_7, M_8 and M_9 as in [26] SN_k sends the authentication reply message to GWN.

Step 4: Do the step of 1 to 3, the messages can be retransmitted up to three times as retrials.

Step 5: Updation of password are done by a legitimate user and also biometric information at any instant completely locally deprived of GWN intervening as and on necessary point.

Step 6: Security checking for the authentication process will be done using UABKMP based ROR model [29]. The three primary participants in this network, namely SN_k, U_i and GWN. Under this model, all communications might be controlled by adversary A including reading and modifying all transmitted messages, and also fabricating new messages as well as injecting them.

Step 7: On receipt of $\{M_9\}$, server computes $h(h(U_i)\|SK_{ji})$ and verifies its equality with received value M_9. If this verification is success, it implies that no replay or forgery is executed and U_i is authenticated finally.

User's Key Change Phase: According to suggested protocol, the user's key can be altered through re-enrollment process. When the key is compromised, U_i can do reenrollment by his/her biometric, and then a new key is generated arbitrarily; this key varies from the previous.

3. SECURITY ANALYSIS

This section explicates security part of protocol and emphasizes the importance of the suggested protocol in terms of

safety. Crypto protocols are evaluated in the threat model because of communication process as interact through an unsafe channel. HIoTNsis implemented on every unsafe, un-trusted end points communication adopting in a threat model

- **DoS Attack**: The recommended protocol is resistant to a DoS assault by pre-authentication, as one in all application are by the U_i's key encryption with timestamp T_1; it meant several requests of unauthorized cannot enters GW node.
- ***Node Compromise Attack***: The recommended protocol resists a node compromise attack as application of the user is first authenticated by GW node and then application is transferred to sensor node to answer user query. The timestamps T_i are used in recommended protocol for replay attack prevention. If an adversary intercepts message $E_K(R,T_1)$ and Attempts to replay the same login message to the GWN, he / she cannot transfer the login request verification due to $(T_2\text{-}T_1) > \Delta T$, where T_2 denotes time when replayed message is received via GWN.
- ***Repudiation Attack***: Denial of participation in every communication is said to be Repudiation attack. For regeneration of U_i's key iris U_t's is required. Therefore U_i cannot reject their participation in a particular way; we also suppose that the GW node is deemed a node of trust; therefore, the suggested protocol resists repudiation attacks.
- ***A Stolen Verifier Attack***: Attackers with unauthorised GW node user keys is unable to retrieve any helpful data because of encrypted keys in the GW node database.
- ***Node Capture Attack***: The entity selects a random value in the communication authentication process to produce a session key that will be discarded at the end of the session.
- ***Replay Attacks***: If a malicious attacker gets a session key or captures HIoTN's network traffic, it is not valid for the session key to recognize malicious visitors and authenticate their identity. Due to illegal identity, resend message will be discarded.

4. PERFORMANCE COMPARION

The Table.1 parameters are used in the Ubuntu 16.10 operation system, made sensor by grid style at 20 m distance between sensors with an incremental step of 20 sensors from 20 to 120 in quantity. HGWN is present in every simulation and transmits between sensors and users. Speed of 2 m/s is achieved with 400×300 m^2 area among 50 users in the test and reaches 4s in packet sending from user in 1800 s simulation time with random start time and based on NS-3. Furthermore, the presented scheme UABKMP is evaluated by performance comparison with existing scheme UAKMP on simulating results via the famous tool NS-2 based on the parameter metrics of communication overhead, throughput, end-end delay and packet delivery ratio.

Table.1. Basic Parameters in Simulation

Description	Value
Area for sensors	400×100 m^2
Number of users	50
Number of sensors	120
User speed	2 m/s
Area for users	400 × 300 m^2
Simulation time	1800 s

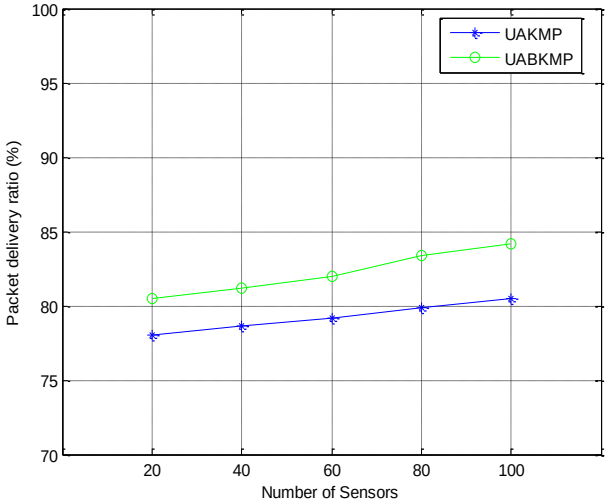

Fig.4. Packet Delivery Ratio vs. No. of sensors

The number of delivered and transmitted messages to the user is referred to as packet delivery ratio is as Fig.4. It usually portrays the message state sent to the destination node. In comparison to the simple UAKMP approach, the proposed UABKMP achieves a high level of packet transmission. From the Fig.4, when the number of users increases, the appropriate delivery ration also increases gradually. When the user value is 50 and the corresponding PDR of UABKMP is 84%, and the existing UAKMP is 3% less effective than the proposed work, the proposed work is more effective for HIoTN. The reason is that the proposed work can identify trustworthy users in its neighborhood.

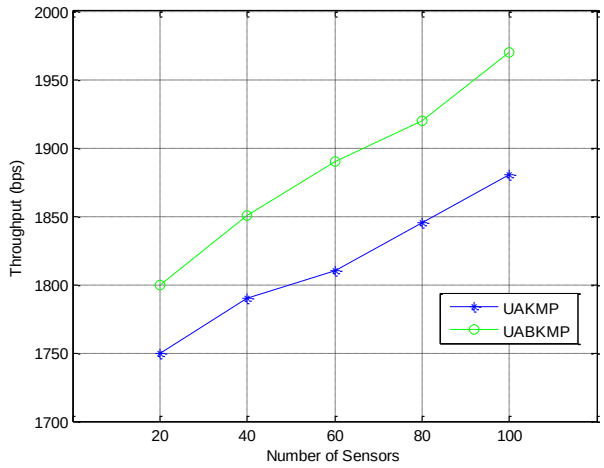

Fig.5. Throughput vs. No of sensors

The Fig.5 shows the comparison result of throughput from the proposed UABKMP, and the existing UAKMP method. It is noted that the proposed UABKMP attains higher throughput when related with prevailing UAKMP. The throughput performance by nodes is perceived to be still higher for further increasing nodes too. The proposed UABKMP has throughput rate of 1962.26bps at the sensor size of 120 when comparing with existing UAKMP

providing low throughput results which is 130.26bps lesser than the suggested method. The purpose is that, suggested work has the capable of identifying malicious nodes in a good biometric authentication system which leads the throughput would be higher.

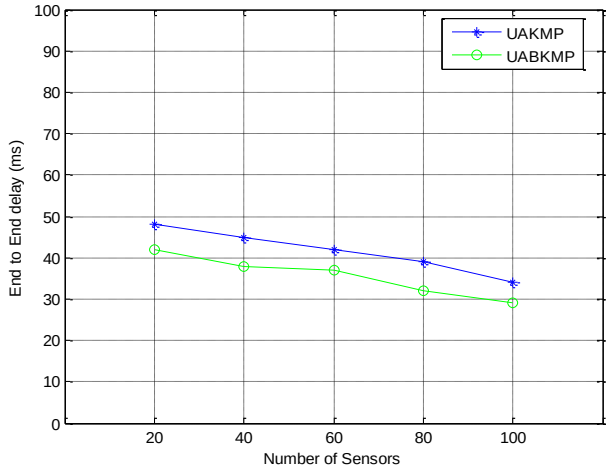

Fig.6. EED vs. No. of sensors

The comparison results of the end-to-end delay between the proposed UABKMP, and the existing UAKMP scheme are shown in Fig.6. Moreover, on increasing sensors, delay reduction is caused in the proposed method against existing methods. The proposed UABKMP has a delay rate of 28.21ms at the sensor size of 100 when compared with the existing UAKMP, providing high delay results which is 7.94ms higher than the proposed method. In suggested work, the secret key value is calculated using the ROR model at each layer with respect to attacks. This leads to a less end-end delay in contradiction with the prevailing work.

Communication Overhead: The overall time taken to complete the successful data transmission is defined as End to end delay

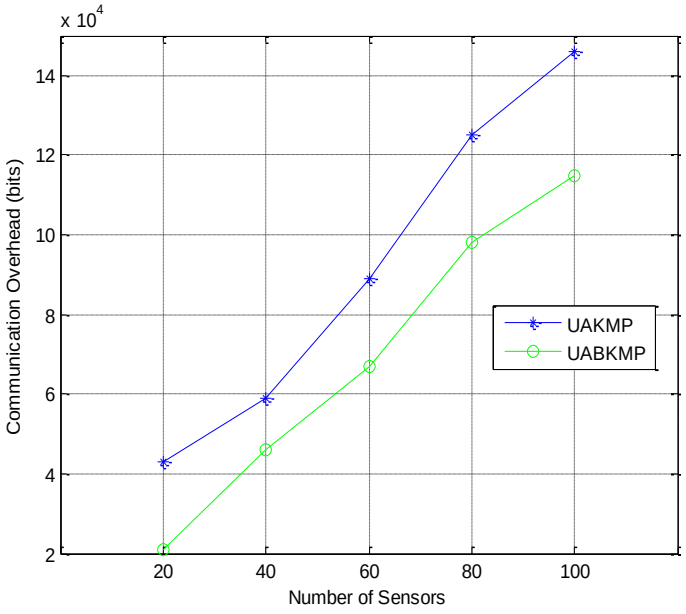

Fig.6. Communication overhead vs. No of sensors

The comparison results of communication overhead between the proposed UABKMP and the existing UAKMP scheme are shown in Fig.6. The proposed method has a low communication overhead rate of 11.75×104 bits at the sensor rate of 100. When comparing the communication overhead rate of the existing method, providing high results of 14.25.5×104bits at the same 100 number of sensors. From the results, the UABKMP is more efficient than UAKMP. As a result, ABKMP possesses low communication bandwidth for the transmission of authentication messages.

5. CONCLUSION AND FUTURE WORK

In HIoTN and in a secure generic IoT networking environment, a user direct accessing of the real-time data from sensing nodes for a specific application is required. A new secure lightweight three-factor remote user authentication scheme is developed for HIoTNs, called User Autric Key Management Protocol (UABKMP). Henceforth, the proposed method UABKMP exhibits a new user authentication scheme against several known attacks by segmenting the iris biometric images for HIoTNs based on hybrid MBO. Examination of informal security analysis for several known attacks inclusive of sensing nodes capture attack and even formal security using extensively accepted ROR model are performed. UAKMP Security is ensured by simulated formal security verification using the broadly-used AVISPA tool as compared to other existing schemes. But in future, incorporation of the proxy decryption functionality can be enhanced for more efficiency and time consumption in key exchange and authentication using a robust method of encryption and forensics.

REFERENCES

[1] D. Maresch and J. Gartner, “Make Disruptive Technological Change Happen-The Case of Additive Manufacturing”, *Technological Forecasting and Social Change*, Vol. 155, pp. 1-15, 2020.

[2] M.E. Ahmed and H. Kim, “DDoS Attack Mitigation in Internet of Things Using Software Defined Networking”, *Proceedings of International Conference on Big Data Computing Service and Applications*, pp. 6-9, 2017.

[3] T. Karthikeyan and K. Praghash, “An Improved Task Allocation Scheme in Serverless Computing using Gray Wolf Optimization (GWO) based Reinforcement Learning (RIL) Approach”, *Wireless Personal Communications*, Vol. 117, No. 3, pp. 1-19, 2020.

[4] S. Kannan, G. Dhiman, and M. Gheisari, “Ubiquitous Vehicular Ad-Hoc Network Computing using Deep Neural Network with IoT-Based Bat Agents for Traffic Management”, *Electronics*, Vol. 10, no. 7, pp. 785-796, 2021.

[5] L. Atzori and A. Iera, “The Internet of Things: A Survey”, *Computer Networks*, Vol. 54, No. 15, pp. 2787-2805, 2010.

[6] M. El Hajj, M. Chamoun, A. Fadlallah and A. Serhrouchni, “Analysis of Authentication Techniques in Internet of Things (IoT)”, *Proceedings of International Conference on Cyber Security in Networking*, pp. 1-3, 2017.

[7] L. Celia and Y. Cungang, “Authenticated Key Management Protocols for Internet of Things”, *Proceedings of International Conference on Internet of Things*, pp. 126-129, 2018.

[8] Steve R. Gunn and Basel Halak, "Lightweight PUF-Based Authentication Protocol for IoT Devices", *Proceedings of International Conference on Verification and Security*, pp. 38-43, 2018.

[9] T. Kothmayr, C. Schmitt, W. Hu, M. Br and G. Carle, "DTLS based Security and Two-Way Authentication for the Internet of Things", *Ad Hoc Networks*, Vol. 11, No. 8, pp. 2710-2723, 2013.

[10] Amiya Kumar, Suraj Sharma, Deepak Puthal, AbhishekPandey and Rathin Shit, "Secure Authentication Protocol for IoT Architecture", *Proceedings of International Conference on Information Technology*, pp. 220-224, 2017.

[11] B. Hong Jin, Walter Guttmann and Dog Seong Kim, "A Framework for Automating Security Analysis of the Internet of Things", *Journal of Network and Computer Applications*, Vol. 83, pp. 12-27, 2017.

[12] J. Jiang and L. Shu, "Authentication protocols for Internet of Things: A Comprehensive Survey", *Security and Communication Networks*, Vol. 2017, pp. 1-18, 2017.

[13] M.N. Aman, M.H. Basheer and B. Sikdar, "Two-Factor Authentication for IoT with Location Information", *IEEE Internet of Things*, Vol. 6, No. 2, pp. 3335-3351, 2018.

[14] P. Gope and B. Sikdar, "Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices", *IEEE Internet of Things*, Vol. 6, No. 1, pp. 580-589, 2018.

[15] N.G. Veerappan Kousik, K. Suresh, R. Patan and A.H. Gandomi, "Improving Power and Resource Management in Heterogeneous Downlink OFDMA Networks", *Information*, Vol. 11, No. 4, pp. 203-216, 2020.

[16] R. Amin, N. Kumar and G.P. Biswas, "A Light Weight Authentication Protocol for IoT-Enabled Devices in Distributed Cloud Computing Environment", *Future Generation Computer Systems*, Vol. 78, pp. 1005-1019, 2018.

[17] Yong Li and Lijun Liao, "Flexible Certificate Revocation List for Efficient Authentication in IoT", *Proceedings of International Conference on Internet of Things*, pp. 1-7, 2018.

[18] P. Mahalle, S. Babar, N. Prasad and R. Prasad, "Identity Management Framework Towards Internet of Things (IoT): Roadmap and Key Challenges", *Proceedings of International Conference on Virtual Local Area Network Technology and Applications*, pp. 430-439, 2010.

[19] K.W. Kim, Y.H. Han and S.G. Min, "An Authentication and Key Management Mechanism for Resource Constrained Devices in IEEE 802.11-based IoT Access Networks", *Sensors*, Vol. 17, No. 10, pp. 1-20, 2017.

[20] G. Dhiman, K. Somasundaram and K. Sharma, "Nature-Inspired-Based Approach for Automated Cyberbullying Classification on Multimedia Social Networking", *Mathematical Problems in Engineering*, Vol. 2021, pp. 1-21, 2021.

[21] P.K. Dhillon and S. Kalra, "Multi-Factor User Authentication Scheme for IoT-Based Healthcare Services", *Journal of Reliable Intelligent Environments*, Vol. 4, No. 3, pp. 141-160, 2018.

[22] M. Wazid, A.K. Das, V. Odelu and N. Kumar, "Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks, *IEEE Internet of Things*, Vol. 5, No. 1, pp. 269-282, 2017.

[23] N.V. Kousik, P. Johri and M.J. Divan, "Analysis on the Prediction of Central Line-Associated Bloodstream Infections (CLABSI) using Deep Neural Network Classification", *Proceedings of International Conference on Computational Intelligence and Its Applications in Healthcare*, pp. 229-244, 2020.

[24] T. Song, R. Li, B. Mei, J. Yu, X. Xing and X. Cheng, "A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes", *IEEE Internet of Things*, Vol. 4, No. 6, pp. 1844-1852, 2017.

[25] A.K. Das, P. Sharma, S. Chatterjee and J.K. Sing, "A Dynamic Password-Based User Authentication Scheme for Hierarchical Wireless Sensor Networks", *Journal of Network and Computer Applications*, Vol. 35, No. 5, pp. 1646-1656, 2012.

[26] P. Johri, "Improved Energy Efficient Wireless Sensor Networks using Multicast Particle Swarm Optimization", *Proceedings of International Conference on Innovative Advancement in Engineering and Technology*, pp. 1-6, 2020.

[27] O.R. Vincent and O. Folorunso, "A Descriptive Algorithm for Sobel Image Edge Detection", *Proceedings of International Conference on Informing Science and IT Education*, pp. 97-107, 2009.

[28] J.H. Lin, C.W. Chou and C.H. Yang, "A Chaotic Levy Flight Bat Algorithm for Parameter Estimation in Nonlinear Dynamic Biological Systems", *Computer and Information Technology*, Vol. 2, No. 2, pp. 56-63, 2012.

[29] M. Abdalla, P. Fouque and D. Pointcheval, "Password-Based Authenticated Key Exchange in the Three-Party Setting", *Proceedings of International Conference on Theory and Practice in Public Key Cryptography*, pp. 65-84, 2005..