International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-6, Issue-7)

Research Article

July 2017

Proposed SMRAC: Secure Medical Record Access Control Model in Wireless Sensor Networks

Navneet Kaur, Sheenam Malhotra
Department of Computer Science and Engineering, Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India

Abstract-

Due to numerous uses of wireless sensor networks in various fields, they have attracted much interest in research community. For the monitoring and surveillance purposes wireless sensor networks are mostly used. In healthcare, WSNs are being popular due to its ease of use because patients can be monitored easily even at their homes by the doctors. A Break-The-Glass Access Control (BTG-AC) model was proposed with more flexible access to medical data in a reasonable time to provide data availability to the users. In the BTG-AC, security of the data never considered. For the security of the data an innovative security approach is desirable that also fit into WSNs. So, a new Secure Medical Record Access Control (SMRAC) Model is proposed. SMRAC is same as BTG-AC model but the main difference is to address the security issue. Parallelizing ciphertext policy attribute-based-encryption is implemented in SMRAC to improve the security of patient's data. Simulation result shows the effectiveness of the SMRAC model. For the further evaluation, SMRAC model is compared with the existing BTG-AC model in terms of fault detection and execution time.

Keywords - WSNs, BTG-AC model, SMRAC model, security, Attribute-based-encryption, Access control, P-CP-ABE.

I. INTRODUCTION

WSNs are being popular in healthcare for monitoring the patients at their homes. Patients have worn sensors that detect their physical conditions such as temperature, heart rate etc. In emergency, patients have to be treated carefully in a reasonable time to avoid the uncertain situation to be happen. In a medical scenario, data should be available every time to the doctors when they need to examine their patients' health condition.

Security and availability both are most important issues in such monitoring systems. WSNs suffer from limited resources, less power, and poor computational capabilities that makes innovative techniques to be followed that can be fit into WSNs and consider their constraints. In healthcare industry, emergency or uncertain situations can be happened at any time. Therefore, data availability should be there to treat patients in reasonable time. For the purpose, an access control model that provides flexible access with required degree of data privacy is required. Data availability should be taken at the most in these kinds of situations but data privacy and data confidentiality should not be neglected. Data security is very much important in such scenario where the users have flexibility to access data in emergency conditions. The access control model should detect the violations from the unauthorized users as well as from the authorized users and an innovative and lightweight access control model is required to avoid the access through the dishonest or malicious users because the security breaches can happen at any time.

Aim of the paper is to implement a lightweight Secure Medical Record Access Control Model same as BTG-AC model but the main difference is to address the security issue, Parallelizing ciphertext policy attribute-based-encryption scheme is implemented in the SMRAC model to provide authentication service to the users and to address the security issue. Parallelizing ciphertext policy attribute-based-encryption is an accelerated ciphertext policy attribute-based-encryption technique in which a user will be able decrypt the data only if that users' attributes pass through the ciphertexts' access structure [8].

Remaining paper structure follows: Section II describes the Literature Review, Section III represents the SMRAC model, Section IV determines results and discussion, and at the end Section V concludes the paper and gives further directions for future work.

II. LITERATURE REVIEW

To address the security policy violations from both the authorized and unauthorized users, a flexible access control model was proposed by Maw et al. [1] named BTG-AC (Break-The-Glass Access Control) model. Availability issue was addressed by the BTG-AC model. But the security of patient data was not considered at the most. The system detects the security policy violations from authorized or unauthorized users but never prevent it from inappropriate user access. For the data privacy and confidentiality an innovative access control model is required to be implemented in WSNs. It cannot be assumed that all the users are trustworthy where large amount of data is going to be shared because security breaches can happen at any time. It is very complex task to secure sensitive and confidential data in WSNs because security technique that works effectively in other wireless technologies cannot directly fit into WSNs because of the resource and power constraints of WSNs. An appropriate and lightweight security approach is required to work effectively in WSNs.

Li et al. [13] proposed a P-CP-ABE scheme to parallelize CP-ABE and port it to multi-core architecture machines. Major performance bottlenecks such as key management and encryption /decryption process are identified and accelerated. AES encryption operation mode was adopted for further performance gains. Experimental results had demonstrated its effectiveness. CP-ABE has become a possible solution to cloud storage. However, its high complexity has prevented it from being widely adopted. Traditional encryption algorithms (both symmetric and asymmetric ones) fail to help achieve effective secure cloud storage due to their severe issues such as complex key management and heavy redundancy. Ciphertext-Policy Attribute Based Encryption (CP-ABE) scheme overcomes the aforementioned issues and provides fine-grained access control as well as deduplication features.

III. SMRAC (SECURE MEDICAL RECORD ACCESS CONTROL) MODEL

In BTG-AC model data availability issue was resolved by allowing users to perform BTG operations to access the data in emergency situations. Data availability has taken at the most than any other security concern in BTG-AC. Security of patient data is very important in such scenario where users are allowed to perform such actions. Data flexibility and efficiency also cannot be neglected. So, an efficient and secure data access model that can be also fit into WSNs is required to make data more secure and available in less execution time. Attribute-based-encryption is widely used efficient encryption technique. Ciphertext-policy-attribute-based-encryption which satisfies the ideal ABE criteria but its high complexity had prevented it from being widely adopted. Using ABE schemes can have the advantages:

- To reduce the communication overhead on the internet.
- To provide a detailed level or fine grained level access control i.e. users in the same group have different access right assigned by the system.

Ciphertext-policy-attribute-based-encryption was first constructed by B. Waters et al. [8] in 2007. In CP-ABE a user's credentials are described by attributes and the party, encrypting the data determines a policy for who can decrypt the data. A user will be able to decrypt the data only if that user's attributes pass through the ciphertext's access structure. ABE allows for implementing fine-grained decentralized access control based on properties or attributes a user has. There is no need for writing detailed user-based policies in advance. It makes ABE in particular interesting for implementing security mechanisms in dynamic environments such as disaster management and healthcare [12]. To reduce the complexity of CP-ABE Li et al. [13] proposed P-CP-ABE (Parallelizing-ciphertext-policy-attribute-based-encryption). Key management and encryption/decryption process was identified and accelerated. Results showed its performance gain and effectiveness.

SMRAC (Secure Medical Record Access Control) model is proposed which is same as BTG-AC model but have main difference is that in SMRAC authentication service is provided by implementing Parallelizing-ciphertext-policy-attribute-based-encryption scheme rather than by using simple login process as in BTG-AC model. Parallelizing-ciphertext-policy-attribute-based-encryption will detect security policy violations and prevents the unauthorized access to data and maintain the data confidentiality and integrity. Confidential data will not be accessed by unauthorized or dishonest users.

A. Steps of SMRAC (Secure Medical Record Access Control) Model

Step 1: Input the rules and policies according to the project. // e.g. for hospital management system, the policies will be fix appointment, bill payment, medical record etc.

Step 2: Define the glass break rules on the basis of functions associated with the authority. // e.g. only doctor has access rights to change medical record.

Step 3: Apply Parallelizing-ciphertext-policy-attribute-based-encryption to increase security of glass break policy and policies are hidden from the users and only visible to those who have their access rights. Step 3.1 to step 3.6 includes the implementation of Parallelizing-ciphertext-policy-attribute-based-encryption scheme in the SMRAC Model. It mainly consists of four major modules: setup, encryption, key generation and then decryption.

Step 3.1: The first step is bilinear mapping of two cyclic groups G0 and G1 of prime order p.

Step 3.2: The users' attribute set S taken as input that generates public key P_k and master key M_k as output.

Step 3.3: Access policy structure of the ciphertext T generates secret key S_k that specifies users' attribute set S by taking M_k and T as input to provide S_k as output to users.

Step 3.4: Ciphertext access structure takes plaintext message M and attribute set S as input and to give ciphertext as output.

Step 3.5: Ciphertext policy takes access structure T, Public key P_k and plaintext M as input and gives ciphertext CT that satisfies users' attributes of set S.

Step 3.6: By using Users' secret key S_k and ciphertext CT, one can decrypt the ciphertext and get plaintext M as output. Otherwise, null if access is denied.

Step 4: All the actions are stored as an audit log and glass broken policies are checked in terms of fault detection and execution time.

B. Flowchart for SMRAC (Secure Medical Record Access Control) Model

Fig. 1 represents the flowchart of the implementation of proposed SMRAC model.

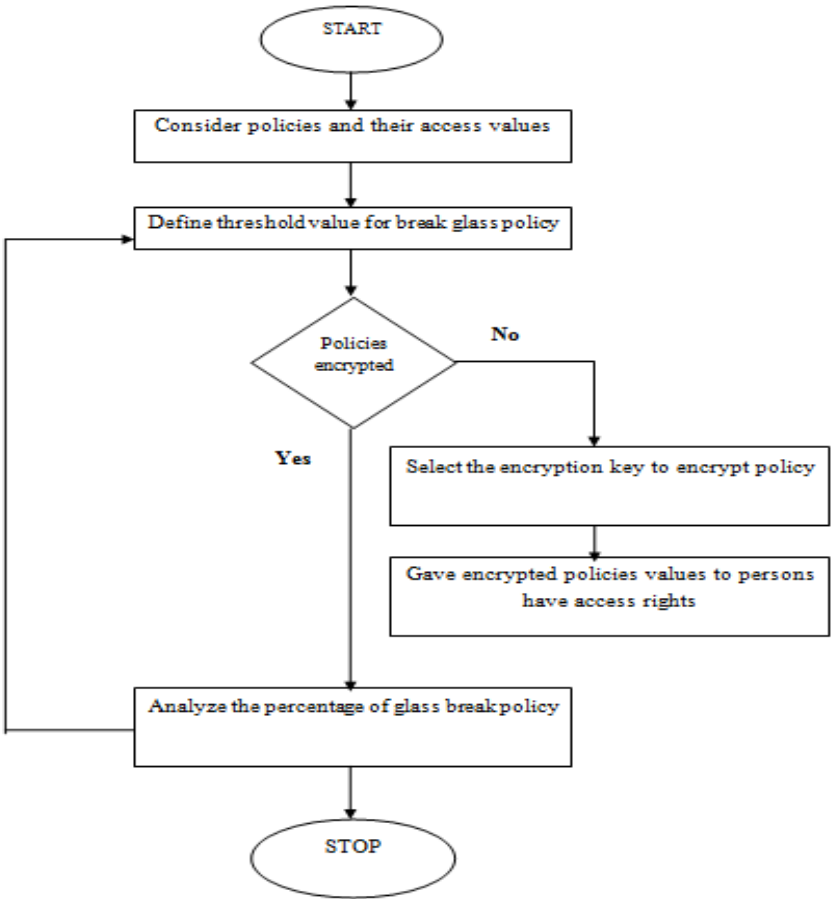

Fig. 1 Flowchart of SMRAC model

IV. RESULTS AND DISCUSSION

Simulation is carried out by using MATLAB simulation tool. Set up simulation environment by randomly deploying sensor nodes. Figure below shows hospital management system scenario for four users: Doctor, Nurse, Staff, and Patient. The users have seven functions: New registration, Fix appointment, Audit, Medical record, Change record, Decision making, and Bill payment. Each user has different predefined policies/access rights according to their roles in the system.

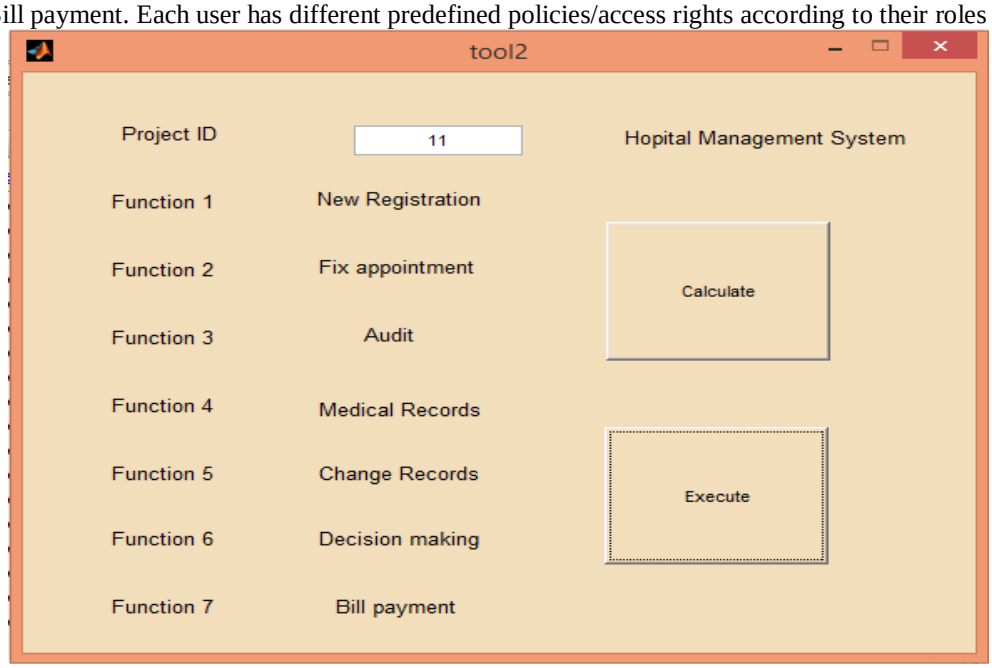

Fig. 2 Functions of hospital management system

In Fig. 3 Policy broken probability (PBP) is calculated to check the importance of the above functions. Function importance shows the execution value of a function. Policy broken probability is given by:

$$PBP = \frac{Policy\ no.}{No.of\ times\ the\ policy\ executed}$$

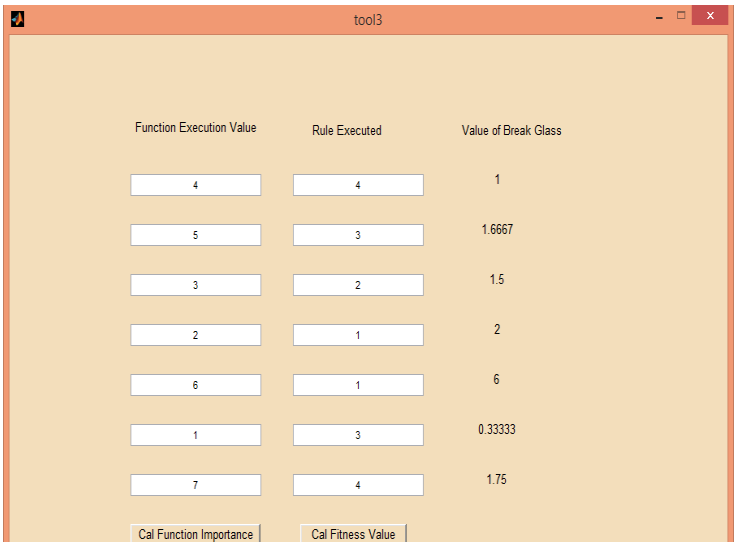

Fig. 3 Policy broken probability

Fig. 4 shows the percentage of break glass at subject 1 is 24%. Average fault detection percentage is 11.0177% in execution time of 9.1815 seconds. Average fault detection percentage is calculated as:

$$AFDP = \frac{total\ no.of\ faults\ found}{total\ no.\ of\ subjects(users)} * 100$$

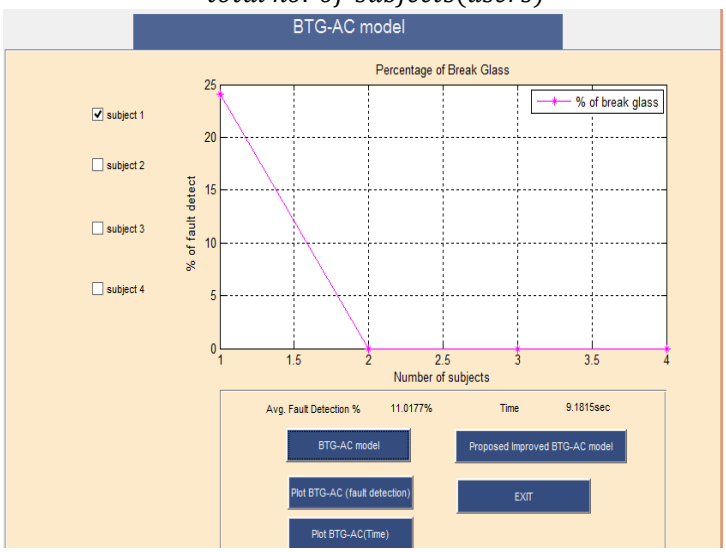

Fig. 4 Existing BTG-AC model

Fig. 5 and Fig. 6 shows bar graphs of Average fault detection % and execution time of BTG-AC respectively.

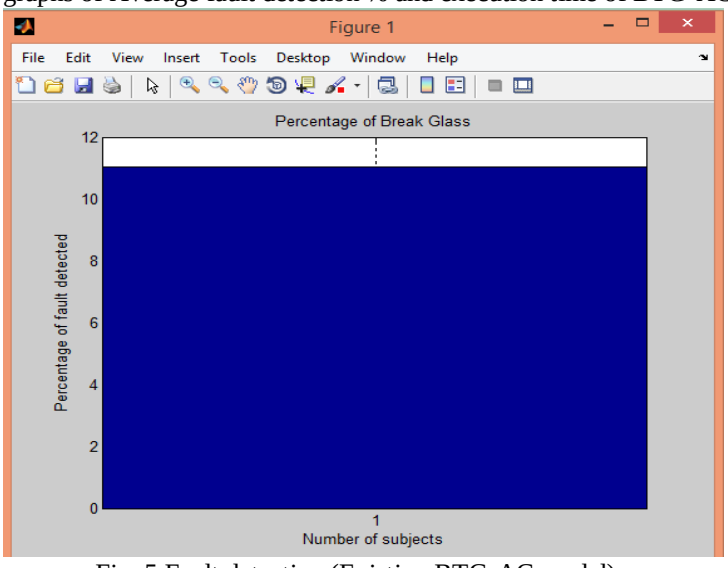

Fig. 5 Fault detection (Existing BTG-AC model)

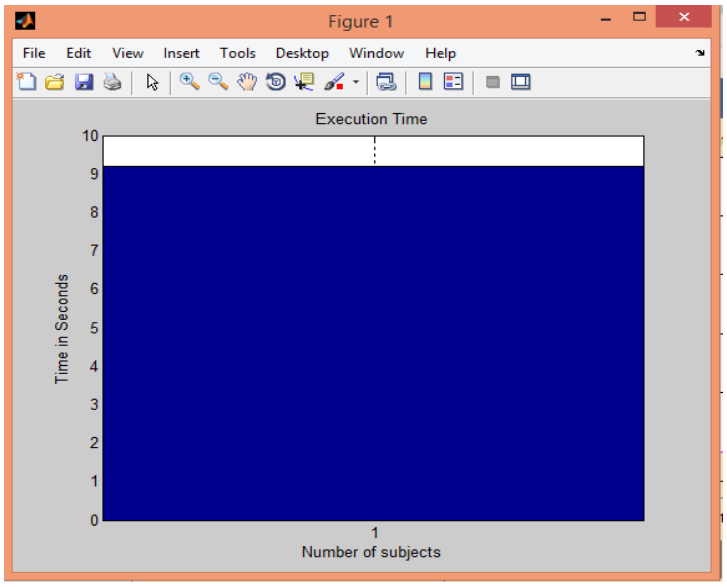

Fig. 6 Execution time (Existing BTG-AC model)

Fig. 7 shows proposed SMRAC model in terms of two parameters: fault detection and execution time. In SMRAC model, Parallelizing-ciphertext-policy-attribute-based-encryption scheme is implemented to address the security issue in access control models where users have the flexibility to break-the-glass to access the data.

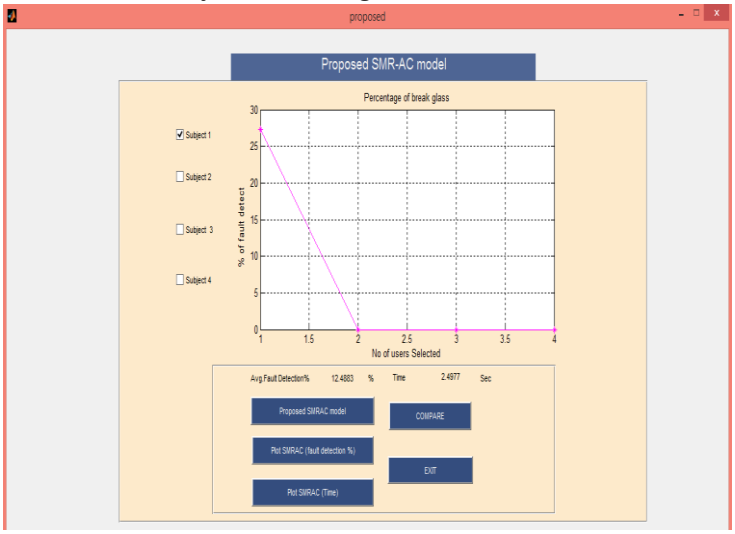

Fig. 7 SMRAC Model

Fig. 8 shows average fault detection percentage given by SMRAC Model. It gives 12.4883% average fault detection rate

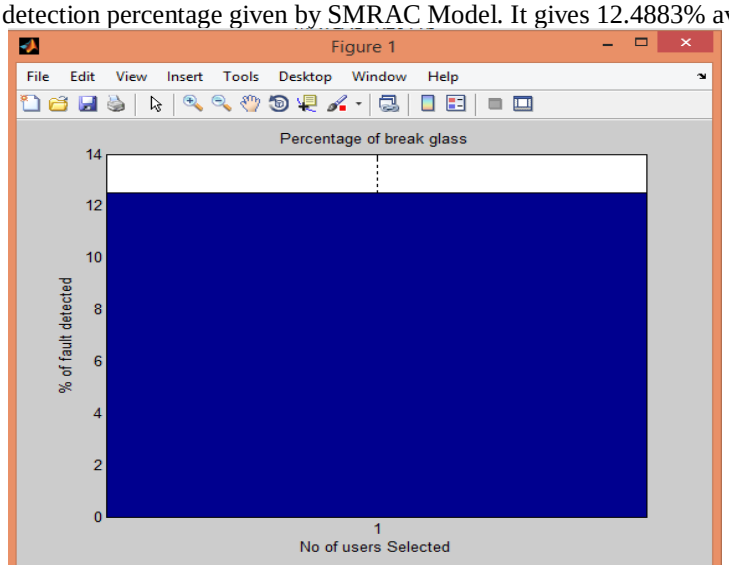

Fig. 8 Fault detection (SMRAC model)

Fig. 9 represents the bar graph of execution time of SMRAC Model.

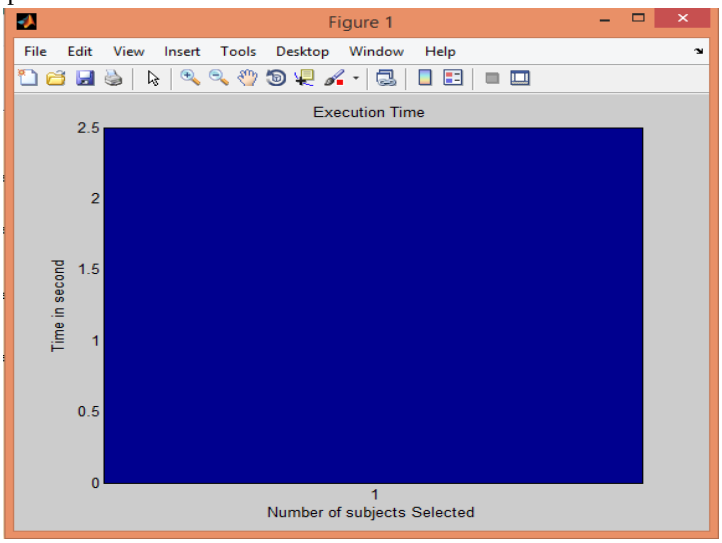

Fig. 9 Execution time (SMRAC model)

Fig. 10 shows the comparison of existing BTG-AC with SMRAC (Secure Medical Record Access Control) Model in terms of execution time. Simulation result shows that SMRAC model outperforms BTG-AC in terms of execution time. In SMRAC model policies are hidden and visible to only those who have the access rights to that policy.

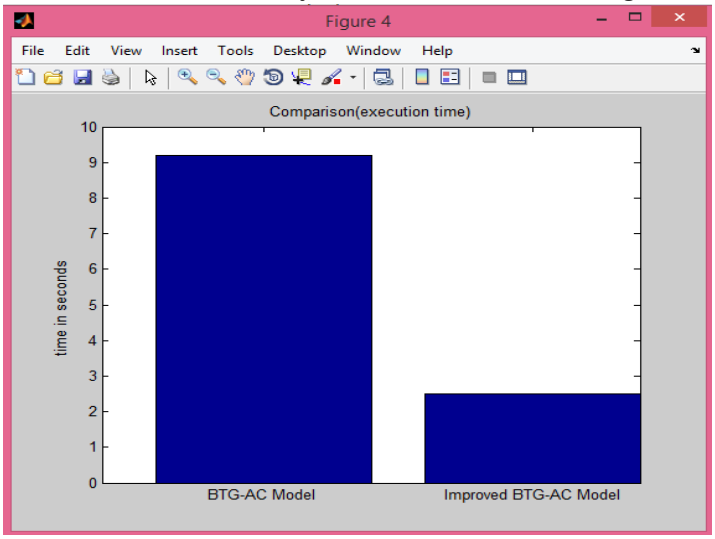

Fig. 10 Comparison (Execution time)

Fig. 11 shows the comparison of existing BTG-AC model and SMRAC model in terms of fault detection. Existing BTG-AC detects 11.01770% average fault detection and SMRAC model detects 12.4883% average fault detection. Implementation of P-CP-ABE in the SMRAC model improves security of the model.

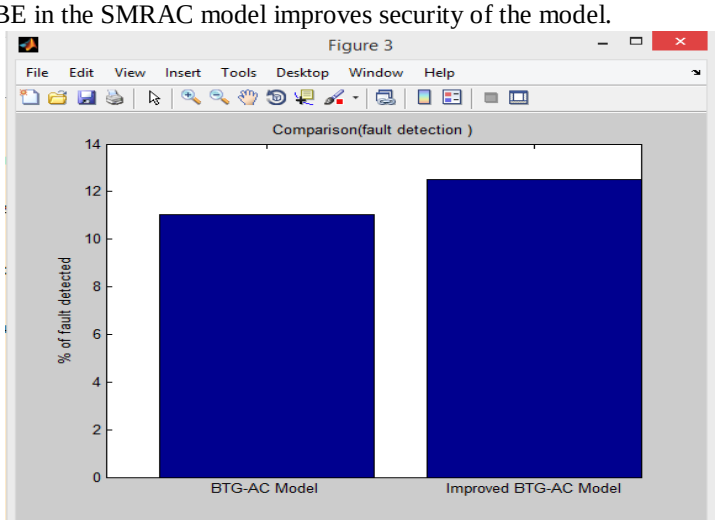

Fig. 11 Comparison (Fault detection)

V. CONCLUSION AND FUTURE WORK

BTG-AC model was developed and implemented in ponder2 to reduce the storage space and to fit into the wireless sensor networks. The existing model addresses the data availability issue. But data security is also very important in such systems that allow flexible access to the users and allow them to perform BTG operations. Attribute-Based-Encryption is well suitable to be used in dynamic environments such as Healthcare because it is used for the fine-grained or detailed level access control that is based on users' properties. Therefore, there is no need to write in detail the user-based policies in advance. So, an efficient and secure SMRAC model is proposed that provides authentication service by using efficient encryption scheme known as Parallelizing-Ciphertext-Policy-Attribute-Based-Encryption to address the security issue of patient data in such scenarios where users have the flexibility to access data by performing BTG operations. At the end of implementation of SMRAC model in MATLAB results are evaluated by comparing its performance in terms of fault detection and execution time with existing BTG-AC model. SMRAC model requires less execution time than BTG-AC and serves security to patient data at fine-grained levels.

In future, human decisions are required to predefine the BTG policy for each object. SMRAC model can be developed within the actual sensor nodes for healthcare applications in WSNs to achieve more efficient and accurate results.

REFERENCES

[1] H. A. Maw, H. Xiao, B. Christianson, and J. A. Malcolm, "BTG-AC Break-The-Glass Access Control Model for medical data in wireless sensor network*," IEEE Journal of Biomedical and Health informatics (JBHI),* vol. 00, pp. 1-12, December 2015.

[2] A. Ferreira, D. Chadwick, P. Farinha, R. Correia, G.Zao, R. Chilro, and L. Antunes, " How to securely break into rbac: the btg-rbac model," *Annual Computer Security Applications Conference (ACSAC),* ISSN: 1063-9527, pp. 23-31, Washington, DC, USA, December 2009.

[3] S. Yu, K. Ren, and W. Lou, "Fdac: Toward fine-grained distributed data access control in wireless sensor networks," *IEEE International Conference on Computer Communications (INFOCOM),* vol. 22, pp. 673-686, Rio de Janeiro, Brazil, April 2009.

[4] H. A. Maw, H. Xiao, and B. Christianson, "An Adaptive Access Control model with privileges overriding and behavior monitoring in wireless sensor networks," *8th ACM International Symposium on QoS and Security for Wireless and Mobile Networks (ACMQ2SWinet),* pp. 81-84, Paphos, Cyprus, October 2012.

[5] H. A. Maw, H. Xiao, B. Christianson, and J. A. Malcolm, "A survey of access control models in wireless sensor networks," *Journal of Sensor and Actuator Networks(JSAN),* issue no. 2,vol. 3, pp.150-180, June 2014.

[6] K. Twidle, E.Lupu, N. Dulay, and M. Sloman, "Ponder2- a policy environment for autonomous pervasive systems,"*IEEE Workshop on Policies for Distributed Systems and Networks,* vol. 00, pp. 245- 246, Washington, DC, USA, May 2008.

[7] A. Jain, K. Kant, and M. R. Tripathy, "Security Solutions for Wireless Sensor Networks," *IEEE 2nd International Conference on Advanced Computing and Communication Technologies,* vol. 00, pp. 430-433, Rohtak (INDIA), January 2012.

[8] J. Bethencourt, A. Sahai, and B.Waters, "Ciphertext-policy Attribute-Based-Encryption," *IEEE Symposium on Security and Privacy,* pp. 321-334, Washington, DC, USA, May 2007.

[9] P. Tiwari, V. P. Sexana, R. J. Mishra, and D. Bhavsar, "Wireless Sensor Networks: Introduction, Advantages, Applications and Research Challenges," HCTL *Open International Journal of Technology Innovations and Research (IJTIR),* vol. 14, pp. 1-11, April 2015.

[10] V. Goyal, A. Sahai, O. Panday, and B. Waters, "Attribute-Based-Encryption for fine-grained access control for encrypted data," *ACM Computing Classification System,* pp. 89-98, Alexandria, Virginia, USA, October 2006

[11] C.C. Lee, P.S. Chung, M.S. Hwang, "A survey on Attribute-Based-Encryption schemes of access control in cloud environments," *International Journal of Network Security (IJNS),* issue no. 4, vol. 15, pp. 231-240, July 2013.

[12] A. D. Brucker, H. Petritsch, and S. G. Weber, "Attribute-Based-Encryption with Break-Glass*," International Federation for Information Processing,* pp. 237-244, 2010.

[13] L. Li, X. Chen, and H. Jiang, "P-CP-ABE: Parallelizing Ciphertext-Policy Attribute-Based-Encryption for Clouds," *17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD),* vol. 00, pp. 575-580, Shanghai, China, May 2016.

[14] Y. Cheng, Z.-y. Wang, J. Ma, J.-j. Wu, S.-z. Mei, and J.-c. Ren, "Efficient revocation in ciphertext-policy attribute-based encryption based cryptographic cloud storage," *Journal of Zhejiang University SCIENCE C (Computers & Electronics),* ISSN: 1869-1951, issue no. 2, vol. 14, pp. 85–97, 2013.

[15] J. Hur, "Improving security and efficiency in attribute-based data sharing," *IEEE Transactions on Knowledge and Data Engineering,* issue no. 10, vol. 25, pp. 2271–2282, October 2013.

[16] J. Li, Q. Wang, C. Wang, and K. Ren, "Enhancing attribute-based encryption with attribute hierarchy," *Springer Mobile Networks and Application*, issue no. 5, vol. 16, pp. 553–561, April 2011.

