An Attribute Based Break-Glass Access Control Framework for Medical Emergencies

Vidyadhar Aski[1*], Vijaypal Singh Dhaka[2], Anubha parashar[3]
[1, 2, 3] School of Computing and Information Technology, Manipal University Jaipur, India
{[1*]vidyadharjinnappa.aski,[2]vijaypalsingh.dhaka,[3]anubha.parashar}
@jaipur.manipal.edu

Abstract.
IoT enabled medical services are now a days gaining the major ground in modern lifestyle management strategies due to the increasing trends of advancements in design and development of a healthcare devices. A growing number of necessities in creating connected environments for effective treatment of a chronic disorder is further adding the objectivity in modern healthcare services. The IoT environments in healthcare paradigm consists of mainly the data acquisition system that captures the data from patient body and data aggregators or the data commuters that transform the physical layer data into the cloud layer data for analysis. This data is made accessible to medical professionals for further analysis and disease prediction from the cloud space. Data in the cloud storage needs to be protected by various encryption schemes from the unauthorized accesses. It is critically important to offer the data and device services timely during emergency situations in healthcare scenarios. In this view, authors designed a light weight access control framework that enables the users to access encrypted data and devices in two modes: attribute oriented access and emergency break-glass access. Normally, a policy-based, multi-layered authentication technique is used in encrypting data and a medical professional who satisfies the policy guidelines can decrypt the data through set of attributes. Whereas, during emergency situations the need of break-glass access arises so as to bypass the access policies and stringent security walls in order to timely access the data by rescue workers. The proposed framework is lightweight and fast as there are minimal calculations are required at device and storage level thus by forming low computational and latency complexities. The proposed model is proved secure against the standard security models and the efficiency is demonstrated through numerous experimentations.

Keywords: Access control mechanism, Internet of Things (IoT) devices, Healthcare, Multilayer authentication, Break-glass.

1 Introduction

The linear growth in smart instruments and embedded technologies have been creating phenomenal impacts in healthcare services in terms of real-time monitoring [1-9], predictive analysis and management of chronic health issues. Normalizing the major issues of any healthcare devices such as wearability and power durability has been the focus of interest for many researchers since near past and the potential level of addresses to solve those issues are being made by the community eventually. Numerous on-demand innovations for deploying energy efficient healthcare devices in daily life for improving the quality of life has been observed. The applications of IoT in

Healthcare services will pervade different horizontals such as smart city, old-age life management, assisted living, smart-rehabilitation and resource utilizations. The IoT absolutely add values to the ecosystem by providing connected environments in the era of opportunities.

IoT is creating a platform for cyberspace which is increasingly stacking up with the heterogynous data collected from seamless devices every day. A recent survey anticipates a fact that every year there are millions of new devices getting registered in various sectors for collecting data for the analysis purpose. Therefore, IoT has gained the interest of many stakeholders from research and development community, industrial fraternity, and the academic researchers. This enables the development of industrial applications at different levels of the organizational hierarchy. On the other hand, the IoT in healthcare sector can be thought of as a growing network of human and wearable sensor devices that creates their visibility through an IP address in the Internet web. Automation in data gathering is nearly feasible in all aspects of healthcare services since IoT is featured by advanced set of wireless connectivity components [6].

One of the main objectives of the IoT enabled health services is to provide its end users a network identity on World Wide Web. This enables the users to access numerous on demand services timely and help the patients to maintain the quality of life through the periodic assessments and regular prescription follow-ups [7]. Further, it adds the offerings of telemedicine services to the subscribed set of users with the help of remote assistance. For instance, a healthcare professional can have an access to all the enrolled patient records stored in the medical server and dispense the prescription details to respected patients based on the conditions. The geographical network expansion is still having many limitations in several developing countries, where Internet access is restricted due to progressing infrastructural designs and poor network reachability. In these places, the remote medical services can be accelerated by distributing the potential IoT and mobility services [8].

Consequently, IoT enabled healthcare services are likely to reduce the wait time of patient wait time and cost of treatment along with the improved user experience. As per the service provider view, it is expected that the device downtime can be slashed down through remote maintenance of such devices via cloud APIs. Overall, IoT enabled healthcare services offers the cutting edge solution to many existing medical issues and improves the quality of life.

Nevertheless, since IoT predicates the open end solutions through wireless communication technologies (WCTs) deployed on conventional internet architecture, there is a high chance of data and service leakages through loopholes in security models. Since the whole architecture of IoT is connected through world wide networks without a dedicated channel or medium, the healthcare sector might become a target for unprofessional hackers. The data collected from individual devices through WBANs is vulnerable to the third party demodulation schemes [9, 10]. In addition, unauthorized accesses to healthcare devices would create irreversible security breaches in the healthcare services with the consequent deaths at worst case. Hence, the misuse and security issues of healthcare devices may create a negative impact on diversifying the IoT use cases in healthcare industry. In order to prevent such misusages of healthcare devices and data, many access control mechanisms are already in place providing security support to the

data and devices. Access controlling can be achieved in many ways including attribute based and attribute based authentication. The aim of these authentication protocols is to validate and verify the legitimacy of the user based on the predefined policies and roles within the system.

However, the complexities of multilayered authentication and access control algorithms is significantly high due to the recurrent executions of processes within the main process. Therefore, handling emergency situations with these algorithms is as difficult as breaking a multilayered security model. For instance, a patient suffering from cardiovascular disease who use an IoT device for his regular monitoring of bio-parameters such as heart rate, ECG etc. may undergo a sudden cardiac arrest and loses the cognizance and he is not able to grant access rights to the device or spot rescuers. This may create significant delay in hospitalization and would even lead to death of the patient. In these situations, it's critical to gain the data/device access and work towards the first aid rescuing of patient [8]. In this regard, authors present a break-glass access control framework suitable for issuing the quick access rights to the emergency situation handlers so that we can avoid consequent causalities. Here, break-glass intuitively refers to the information that this algorithm executes only during emergency situation and transfer the access rights to someone who's registered as an emergency situation handler bypassing the actual policies of normal access control scheme. Due to the fact that this break-glass mechanism overrides the access control policy, it should not be used for wrong intentions thus the authority transfer will be done under controlled environment.

2 Existing work and motivation

The Access controlling in IoT enabled ubiquitous medical services have been a key point of discussion for many researchers ever since the inception. Disruptive technologies such as Block chain computing and Big data analytics under the light of IoT have been key contributors in expanding healthcare services to the next level. Several researchers produced high quality outputs in terms of securing, optimizing space constraints and energy optimizations of IoT devices and services recently. In this section, authors discussed few of such research works.

Recently several researchers [9-12] proposed an attribute based access control (ABE) scheme for securely managing data outsourcing applications such as electronic health records (EHR) with enforcement of access control policies and consumer revocation abilities. Most of them employed a mechanism of realizing revocations within a revocation of key attributes. In addition, another ABE was proposed by Narayan et al. [13] for EHR, in which the patient's health data was directly encrypted with a single revocation. Number of non-revoked consumers used to influence the linear growth of ciphertext length though. However, numerous common deficiencies were observed from the aforementioned state-of-art such as the single trusted authority (TA) was used at the time of encryption. Such TAs would cause the system not only a bottleneck problem, but also create the key exposure problems since single TA can have overviewed access to all the encrypted health records and hence this would act as a single door for

exploiting the secured data. In addition, delegating attribute management related tasks to single TA is not at all practical due to the openness nature to vulnerabilities. Further, several of current research works do not specify the attribute dimensions for public and private domains separately since the structure of these domains differ in terms of size of the organizations, and key management strategies. It was also observed from the abovementioned ABE schemes that they have not deliberated any scheme for dealing with emergency situations in healthcare scenarios.

Later, many researchers started including break-glass mechanism in their ABE schemes in order to address the emergency issues in healthcare domain. In 2011, Marinovic et al. [14] proposed an ABE integrated with break-glass access control scheme termed Rumpole supported by declarative query language for specifying the emergency break-glass decision rather than using an implicit predefined decision. Further, attribute-based access control mechanisms embedded with break-glass scheme was proposed by Ming et al. [15] for encrypting patient health records (PHR). In this scheme, the key distribution complexity is reduced by the entire system is divided into multiple security blocks in which each such block manages only the users related to corresponding blocks. However, many of these break-glass control schemes possess only the identity based encryption rather than providing fine-grained access control on the shared ciphertext environments.

2.1 Limitations and emergency constraints enforcement strategies in ABE

Although, there are few researchers as discussed in above section, who lime-lighted their focus on break-glass decryption schemes in access control context, minimal attention has been paid through defining emergency constraints. Such schemes are likely to be misinterpreted at various levels. Though there have been efforts from various researchers in creating the role-based and attribute-based encryption schemes [3-12] ensuring security for EHRs stored in a central server, these schemes fail to produce enough evidences to protect data stored against distributed environments. Along with that defining the emergency constraints in designing break-glass decryption strategies plays a vital role in transferring the authorization during emergency situations. Lack of a schematic authorization scheme for IoT-based medical device can cause life threatening adversarial situation and may lead to death.

3 Proposed architecture and Experimental Setup

The proposed system architecture mainly comprises the group of medical service providers (***MSP***), cloud infrastructure (***CI***), medical service consumer (***MSC***) and emergency situation handlers (***ESH***). Each of these constituents interacts with each other concerning their responsibilities. Fig. 1. Shows the overall system elementary architecture and the corresponding interactions between them.

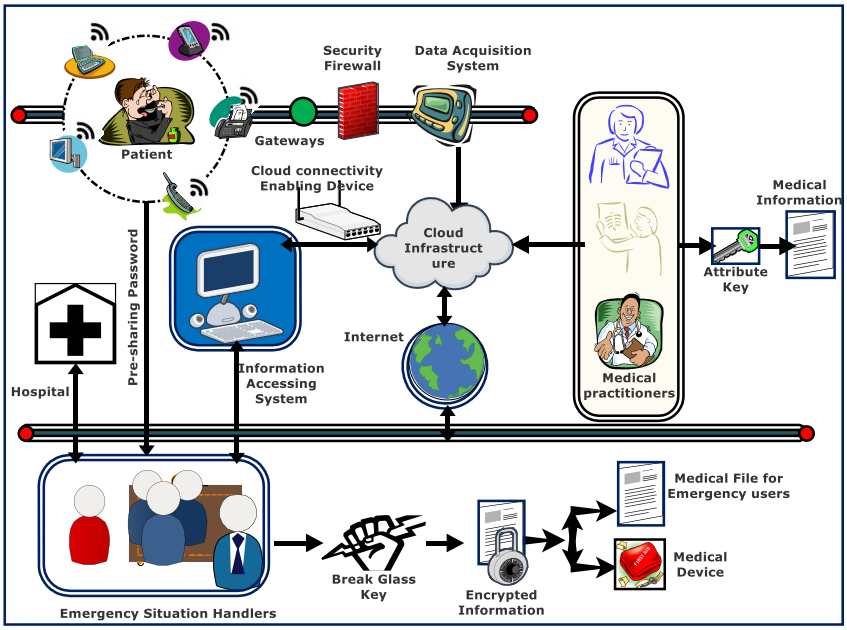

Fig. 1. Overall architecture of the proposed framework

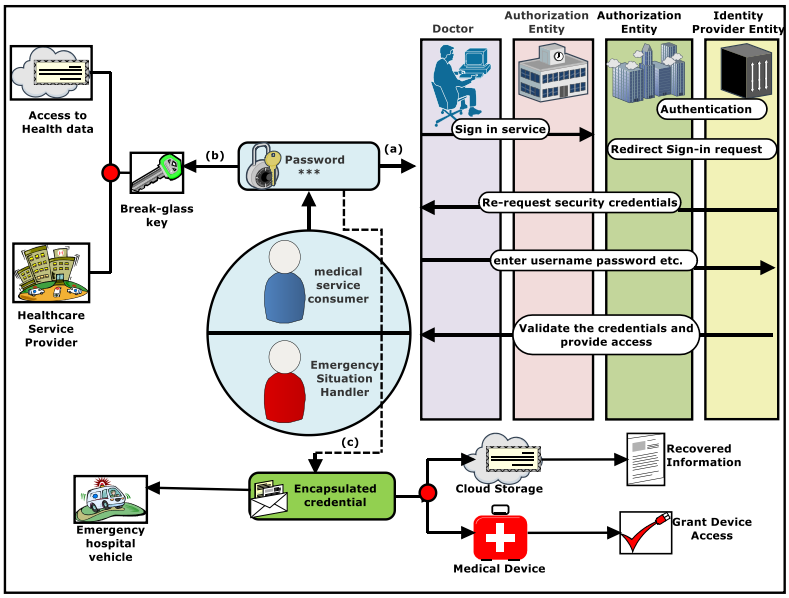

Fig. 2. Generation and extraction of Keys (a): User authentication and generation of emergency session key (ESK) during emergency, (b): Accessing hospital resources by user, (c): ESH care

Key generator is used to create a master secrete key pair for entire scheme and this key will be attributed for the service and data users. The ***CI*** offers the abundant storage and computation space to the consumers and related users. ***MSPs*** are the elementary entities of the proposed scheme, who provides the numerous services to its patients. ***MSC*** gets the services offered by the ***MSP***. Fig. 2 illustrates the generation of break glass encrypted key while verifying the user and his emergency situation for avoiding false alarm servings. The patient needs to set the password ***Pw*** for viewing health data.

Fig. 3 demonstrates the procedural algorithmic representation of proposed scheme. Initially the patient shares the password (*pw*) for accessing his device and cloud data with the registered ESH. The ESH verification is done at the outer layer of the ***BG.KeyExt*** procedure. The peripheral function is attributed by ESH user credentials (cr1, cr2) such as email and resource access password etc. Once the credentials are verified at the CI database, then the legitimacy of the ESH user is identified. This step is to ensure the proposed security scheme cannot be used for misusing. In order to protect *pw*, ESH user utilizes the *pw* in peripheral function and generates encrypted password called emergency session key (ESK) as shown in Fig. 3. The attribute based access the users employs the different attributes such as *session key*, *UI*, *DoB* etc. The Authors invoked attribute based encryption-decryption scheme from [16] in order to utilize time effectively in emphasizing the design of break-glass access. Once the ESH gets the encrypted password EmSesKey, the same is attributed in inner function ***fun2*** along with ***pw*** as shown in Fig. 3. The ESH

```
Password-processed Break-Glass Key Extraction:BG.KeyExt
fun1 Peripheral _ Login.Service (cr1, cr2);

if (authorized!) in Peripheral_Login.service then
    return Error "Invalid ESH"
else
    return EmSesKey
    begin fun2  BG.KeyExt (Pw, EmSesKey)
    Input: Pre-shared patient password  (Pw), Emergency Session Key ( EmSesKey )
   Output: Decrypted Electronic Health Record (Dec.EHR)
    if  EmSesKey in False_Alarm_Entity then
     return  Error "This is a false Emergency!"
   else
      Dec.EHR ⟵new  Dec.EHR.Instance();
      Dec.EHR.add(Pw, EmSesKey);
     Role⟵getRole(uID,DoB);
     ESH-Policies⟵get.ESH.Policy(Role)
     for ESH_policy in ESHpolicies do
         for access_right in ESH_policy do
             //provide access rights for cloud EHR data
             // Provide access to the Medical device (MD)
         end
     end
    return Auth(Bg.Key);
  End
```

Fig. 3 Algorithmic illustration of overall scheme

user will be enabled to access the data and device after the emergency situation occurrence is validated implicitly. Thereafter, ESH user has an access to view decrypted data and device.

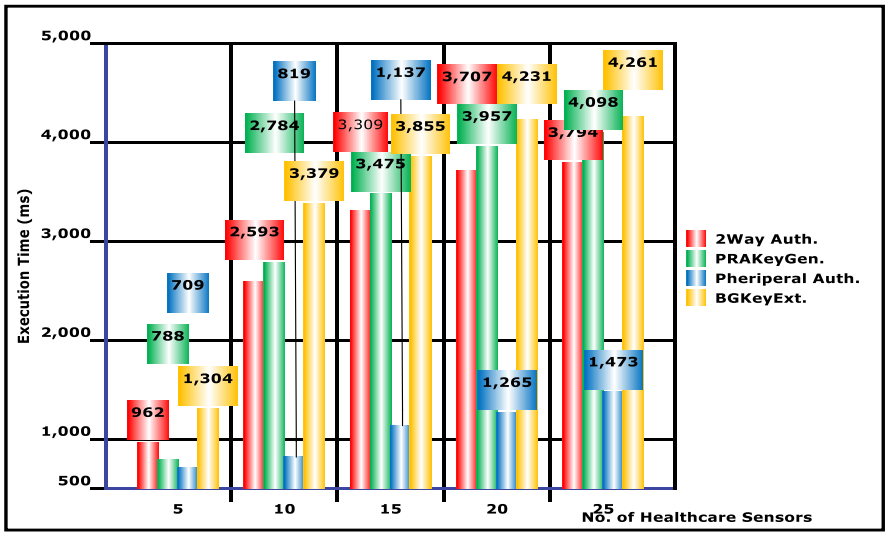

Fig. 4. Comparison of computational complexities of various access control schemes

4 Result Analysis and conclusion

Fig. 4. Illustrates the comparison matrix for computational complexities of various attribute based encryption schemes and the proposed scheme. Authors demonstrated the results with an inclusive architectural manner which comprises of 2 way authentication (2 way auth.), PRAKeyGen [16], peripheral authentication (peripheral auth.) and break-glass key extraction. All these were compared in terms of execution time and observed the better efficiency of proposed scheme. When the no. of resources are high (say more than 25), the multilayer authentication schemes would take more time in executing the tasks. Proposed scheme employs lightweight encryption technique and it can be utilized in the frameworks of any resource constraints devices.

In this article, authors proposed an attribute oriented lightweight secured access control scheme for emergency medical conditions with break-glass capabilities. The scheme can be used to decrypt the data and device in normal mode with the set of attributes, as well as in emergency mode. During emergency mode, the patient predistribute the password for the set of registered ESHs and the same password can be used as an attribute to extract the break-glass key. Once the ESH is successfully verified, he/she will be able to decrypt the EHR data from CI along with having an access right to operate healthcare data. On the basis of Decisional Bilinear Diffie-Hellman (DBDH) hypothesis, the medical data is exhibits resistivity against chosen plain text attack. Thus the proposed model is suitable to be installed in IoT healthcare networks.

References

1. Verma, Prabal, and Sandeep K. Sood. "Fog assisted-IoT enabled patient health monitoring in smart homes." IEEE Internet of Things Journal 5, no. 3 (2018): 1789-1796.
2. Xu, Xiaolong, Shucun Fu, Lianyong Qi, Xuyun Zhang, Qingxiang Liu, Qiang He, and Shancang Li. "An IoT-oriented data placement method with privacy preservation in cloud environment." Journal of Network and Computer Applications 124 (2018): 148-157.
3. www.idc.com, Finding success in the new IoT ecosystem: Market to reach $3.04 trillion and 30 billion connected things in 2020, http://www.idc.com/ getdoc.jsp?containerId=prUS25237214, 2014.
4. Gonizzi, Pietro, Gianluigi Ferrari, Vincent Gay, and Jérémie Leguay. "Data dissemination scheme for distributed storage for IoT observation systems at large scale." Information Fusion 22 (2015): 16-25.
5. Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." Future Generation Computer Systems 82 (2018): 395-411.
6. Khera, Mandeep. "Think like a hacker: Insights on the latest attack vectors (and security controls) for medical device applications." Journal of diabetes science and technology 11, no. 2 (2017): 207-212.
7. Sametinger, Johannes, Jerzy W. Rozenblit, Roman L. Lysecky, and Peter Ott. "Security challenges for medical devices." Commun. ACM 58, no. 4 (2015): 74-82.
8. Aski, Vidyadhar, Sanjana Raghavendra, and Akhilesh K. Sharma. "An Efficient Remote Disaster Management Technique Using IoT for Expeditious Medical Supplies to Affected Area: An Architectural Study and Implementation." In XVIII International Conference on Data Science and Intelligent Analysis of Information, pp. 156-166. Springer, Cham, 2018.
9. Hur, Junbeom, and Dong Kun Noh. "Attribute-based access control with efficient revocation in data outsourcing systems." IEEE Transactions on Parallel and Distributed Systems 22, no. 7 (2010): 1214-1221.
10. Bethencourt, John, Amit Sahai, and Brent Waters. "Ciphertext-policy attribute-based encryption." In 2007 IEEE symposium on security and privacy (SP'07), pp. 321-334. IEEE, 2007.
11. Ostrovsky, Rafail, Amit Sahai, and Brent Waters. "Attribute-based encryption with non-monotonic access structures." In Proceedings of the 14th ACM conference on Computer and communications security, pp. 195-203. ACM, 2007.
12. Boldyreva, Alexandra, Vipul Goyal, and Virendra Kumar. "Identity-based encryption with efficient revocation." In Proceedings of the 15th ACM conference on Computer and communications security, pp. 417-426. ACM, 2008.
13. Narayan, Shivaramakrishnan, Martin Gagné, and Reihaneh Safavi-Naini. "Privacy preserving EHR system using attribute-based infrastructure." In Proceedings of the 2010 ACM workshop on Cloud computing security workshop, pp. 47-52. ACM, 2010.
14. Marinovic, Srdjan, Robert Craven, Jiefei Ma, and Naranker Dulay. "Rumpole: a flexible break-glass access control model." In Proceedings of the 16th ACM symposium on Access control models and technologies, pp. 73-82. ACM, 2011.
15. Li, Ming, S Yu, Kui Ren, and W. Lou. "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings." In International conference on security and privacy in communication, pp. 89-106. Springer, 2010.
16. Vidyadhar J. Aski, Shashank Gupta, and Bharat Sarkar. "An Authentication-Centric Multi-Layered Security Model for Data Security in IoT-Enabled Biomedical Applications." In IEEE 8th Global Conference on Consumer Electronics (GCCE 2019), IEEE Consumer Electronics Society, Osaka, Japan, Oct. 15-18th, 2019. (Accepted, in Press)