IJRSET APRIL 2017 Volume 4, Issue 4 Pages: 40-46

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

IOT BASED SECURE HEALTH CARE SYSTEM USING BSN

[1] S J Preethi, [2] Dr J Senthil Kumar,
[1] PG Scholar, [2] Professor,
[1, 2] Department Of Information technology,
[1, 2] Sona College of Technology, India.

ABSTRACT: Body Sensor Network (BSN) which can be used mainly for Physiological monitoring (i.e., Blood Oxygenation, Pulse Rate, etc..) IoT based Body Sensor network should be implemented in order to improve security. It is mostly useful for the physicians and the patients for real time monitoring, patient information management and health care management. The security requirements can be satisfied using Attribute Based Encryption (ABE) algorithm. It is an type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes. Here the patient id and name is used for encryption. It should be noted that if the BP rate of a person is less than or equal to 120, it is considered to be normal and the server does not perform any action. When the BP of the person reaches say 130, the LPU will provide a gentle alert to the person through the LPU devices like Phone, tablet, etc.. (e.g. beep tone) to the family members of the person. If the BP rate becomes greater than 145 and there is no one attending the call in family, then the server will contact the local physician. Furthermore, if the BP rate of the person cross 160 and still there is no response from the family member or the local physician then the BSN-Care server will inform an emergency unit of a healthcare center and securely provides the location of the person. Key Authority is needed for this to generate key for security purposes. Thus we propose a secure IOT based modern healthcare system using the BSN Care which can efficiently improve the security.

Keywords: [Patient Health Record (PHR), Attribute Based Encryption (ABE), Body Sensor Network(BSN),Internet of things(IoT).]

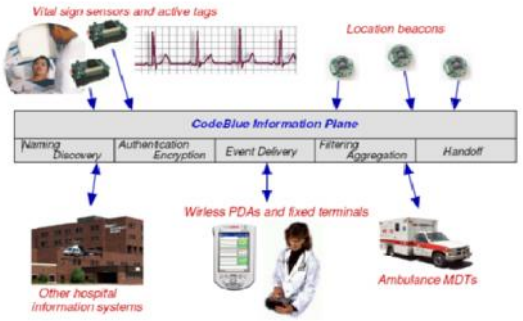
INTRODUCTION

Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," where different services -- such as servers, storage and applications – are delivered to an organization's computers and devices through the Internet. Cloud computing is comparable to grid computing, a type of computing where unused processing cycles of all computers in a network are harnesses to solve problems too intensive for any stand-alone machine.The cloud enables the data centre to operate like the Internet and computing resources to be accessed and shared as virtual resources in a secure and scalable manner. Like most technologies, trends start in the enterprise and shift to

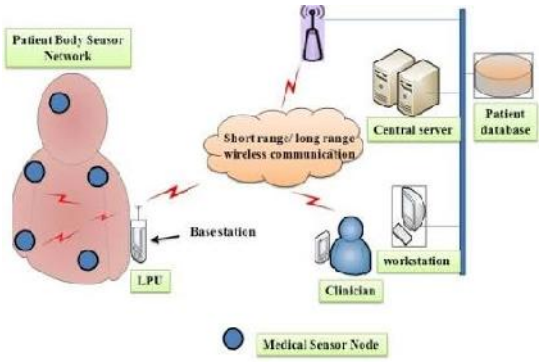
adoption by small business owners. The BSN based healthcare system is mainly used to automatically monitor the patient health condition and information management using a wearable or implanted sensors and then transmit it to the end user device. It consists of security and privacy issues which should be taken into consideration. BSN uses two types of sensor networks to transmit it to the end user device and they are In-body Sensor and On-body Sensor. The security requirements are characterized into Network and Data security. To achieve the security requirements used this Lightweight Anonymous Authentication Protocol and OCB Authenticated Encryption Mode. The Security is not considered as an imperative aspect and thus it makes patient privacy vulnerable. In this paper produce A secure IOT based healthcare system is proposed for patient health monitoring and information management which is called as BSN-Care. The security requirements such as Network and data security is developed using some protocol named as Attribute Based Encryption (ABE). Advantages of Data transmitted to the end user are considered to be more secure. It reduces the computational time and execution time.

RELATED WORK

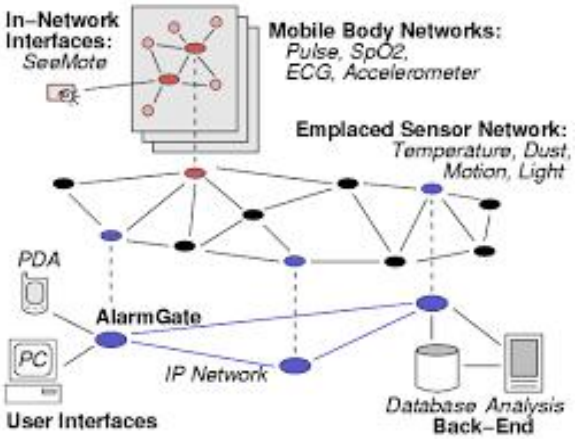
Code Blue: An ad hoc sensor network infrastructure for emergency medical care says Code blue uses Wearable sensors to monitor the patients' health condition and can store patient data like identification, history and treatments. In a mass casualty event (MCE), sensor networks can greatly improve the ability of first responders (i.e A person who can help to dispatch to ambulance) to treat multiple patients equipped with wearable wireless monitors. Code Blue is based on a publish/subscribe model for data delivery, where the nodes can publish data of location and identities where the physicians and nurses can subscribe.



Ubiquitous Monitoring Environment for Wearable and Implanted Sensors: It shows the aim of having aUbiMon for wearable and implantable sensors is to provide continuous management of patients under their natural physiological states. The system is mainly used for collecting, gathering and analyzing data from number of sensors



ALARM-NET: WSN for assisted living and residential monitoring says ALARM-NET is used mainly used for assisted-living and residential monitoring. It integrates environmental and physiological sensors which allow real time collection and processing of sensor data.



Modularity Technology in Manufacturing: Taxonomy and Issues this paper presents taxonomy on modularity applications, research issues, and design methodologies. The General framework for further systematic development of modularity in systems this technique are used. A general framework for architectures of modular systems was proposed, architectures of existing modular systems can be analyzed. One of the particular points is the recognition of the so-called coordination concept in this general framework.There is a generic computational procedure for developing a modular architecture for an existing system. However, this computational procedure does not appear able to produce a specific modular architecture within the general architecture of modular systems. A preliminary thought would be that the framework components (e.g. component swapping, components sharing, etc.) of the general framework are not on the same level of activities defined in the generic computational procedure. In particular, the activities which would help to produce a specific architecture which contains those framework components may follow activities in the generic computational procedure.

Automated sequencing and sub-assembly detection in automobile body assembly planning shows the possible sub-assemblies are automatically detected by satisfying some mathematical conditions applicable to these matrices. The Genetic algorithms are used in this project. The advantage is distinguishing the physical connection and non-contact constraints in a connection matrix. Because most components of an automobile body have complex shapes, the non-contact constraints are the common precedence knowledge in automobile body assembly sequence planning. It Detecting all the possible sub-assemblies in order to simplify the sequence generation phase and in some cases, to enable the assembly of the product. The disadvantages are generating all the possible sequences. The possible sub-assemblies are automatically detected by satisfying some mathematical condition applicable to the connection matrix and contracted matrix.

Disassembly matrix for disassembly processes of products shows the proposed disassembly matrix provides more possible disassembly processes than the existing disassembly methods to determine preferred disassembly processes.Depth-First-search algorithm is used this project. The advantages are Application of the results from this study will reduce human errors during determining disassembly processes. Importantly, by applying the methodology described in this study, disassembly sequences for complex devices will dramatically improve.Some limitations exist and the software needs to be enhanced in this study, the proposed disassembly matrix needs a smaller computer memory than that of the Dini and Santochi method.And it can also determine all the disassembly sequences and directions of components to improve the existing methods.
Designing Effective Step-By-Step Assembly Instructions shows Algorithmic techniques used to produce assembly instructions given object geometry, orientation, and optional grouping and ordering constraints on the object's parts.Sophisticated low-level algorithmsdescribed a set of design principles for designing effective assembly instructions that are easy to understand and follow. The principles are based on cognitive psychology research examining how people mentally represent and communicate the process of assembling an object. The limitations are System is based on this idea and considers both problems in parallel as it is designing the instructions.

Reconfigurable manufacturing systems: the state of the art is the production paradigms which apply these strategies are also classified. Particular emphasis is put on the paradigm of Reconfigurable Manufacturing System(RMS).

Platform protocol is used the strategies to meet the requirements of a manufacturing system have been generalized, and these

strategies can be used to compare and distinguish various manufacturing paradigms and enabling technologies. It is seen that the RMS paradigm is one of the most effective paradigms to meet some key requirements such as changes and uncertainties.

It is not the complete solution to meet all of manufacturing requirements. To our knowledge, no attempt has been made to combine an RMS with other production paradigms. Many prototype systems have been developed. Most of them are machine-level systems. These systems have been designed intuitively. A systematic design methodology is still lacking.

SYSTEM MODEL

Concert assesses the compliance of a workflow by analysing the five established elements required to check for rule adherence in workflows: activities, data, location, resources, and time limitation. A rule describes which activities may, must or must not be performed on what objects by which roles. In addition, a rule can further prescribe the order of activities, i.e.which Activities have to happen before or after other activities. The formalization of rules as Petri nets patterns has been proposed by Catt et al. And Huang and Kirchner. In contrast to Catt et al., Huang and Kirchner cannot cope with the expression of usage control policies. Catt et al. employ Usage Control Colored Petri Nets (UCPN) for the formalization and enforcement of diverse types of obligations, i.e. actions to be performed before, during and after an activity. However, their approach assumes that the rules are integrated into the workflow, so that UCPN cannot be singled out for reuse for other workflows. Acting as a security automata, rules in Concert are captured as Petri net patterns and are not integrated into the workflow. Together with the classification of compliance requirements, this makes it possible to organize compliance rules in categories according To their intent and semantics, thereby facilitating their formalization as Re-usable Petri net patterns or templates in other modular policy languages for usage control.

ADVANTAGES

As well as contrast our scheme on the way to numerous preceding ones within complexity, scalability and security. Also exhibit the effectiveness of our method via employing it on a current workstation and performing experiments/mode.

SYSTEM MODULES

Login
Registration
Key Authority
LPU
BSN Care Server.

LOGIN

It is used to get access to an operating system or application, usually in a remote computer. It consists of the following (1) a user ID and (2) a password. If the user ID and password is correct then it is directed to Administration page.

REGISTRATION

In this module, Patient's, Physician, Family and Emergency care personal details such as, Name, Contact No will be stored and ID will be given to the everyone. Determining whether the person has been previously registered by searching a database and reviewing possible matches.

KEY AUTHORITY

These are key generation centers that generate public/secret parameters. The key authorities consist of a central authority and multiple local authorities. It assume that there are secure and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase. Each local authority manages different attributes and issues corresponding attribute keys to users. They grant differential access rights to individual users. The key authorities are assumed to be

honest-but-curious. That is, they will honestly execute the assigned tasks in the system , however they would like to learn information of encrypted contents as much as possible.

LPUIn our BSN-Care system, when a LPU wants to send the periodical updates to BSN-Care server, then the server needs to confirm the identity of LPU using a lightweight anonymous authentication protocol. After authenticating the ID , the LPU and server interact with each other.

BSN CARE SERVER

The BSN-Care server receives data of a person (who wearing several bio sensors) from LPU, then it feeds the BSN data into its database and analyzes those data. It may interact with the family members of the person, local physician, or even emergency unit of a nearby healthcare center. BSN-Care server maintains an action table for each category of BSN data that it receives from LPU.

TECHNIQUES AND ALGORITHM

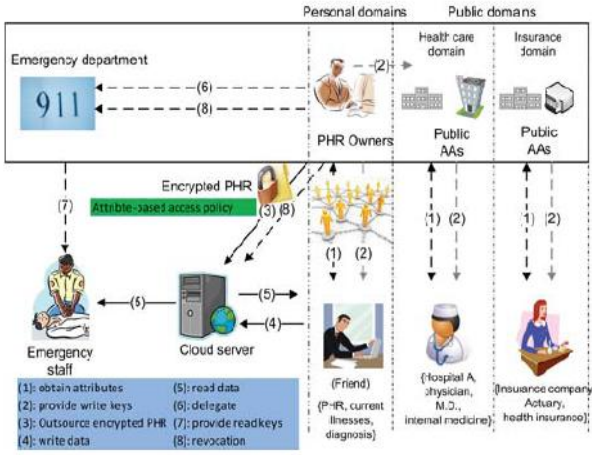
Attribute Based Encryption (ABE)Functional encryption presents a vision for public key cryptosystems that provide a strong combination of flexibility, efficiency, and security. In a functional encryption scheme, cipher texts are associated with descriptive values x, secret keys are associated with descriptive values y, and a function $f(x, y)$ determines what a user with a key for value y should learn from a cipher text with value x. One well-studied example of functional encryption is attribute-based encryption (ABE), first introduced, in which cipher texts and keys are associated with access policies over attributes and subsets of attributes. A key will decrypt a cipher text if and only if the associated set of attributes satisfies the associated access policy. There are two types of ABE systems: Cipher text-Policy ABE (CP-ABE), where cipher texts are associated with access policies and keys are associated with sets of attributes, and Key-Policy ABE (KPABE), where keys are associated with access policies and cipher texts are associated with sets of attributes.To achieve desired flexibility, one strives to construct ABE systems for suitably expressive types of access policies over many attributes. Current constructions allow Boolean formulas or linear secret sharing schemes as access policies. This high level of flexibility means that keys and cipher texts have rich structure, and there is a very large space of possible access policies and attribute sets. This presents a challenge to proving security, since a suitable notion of security in this setting must enforce collusion resistance, meaning that several users should not be able to decrypt a message that none of them are individually authorized to read. Hence a security proof must consider an attacker who can collect many different keys, just not a single one that is authorized to decrypt the cipher text.

Concert assesses the compliance of a workflow by analysing the five established elements required to check for rule adherence in workflows: activities, data, location, resources, and time limitation. A rule describes which activities may, must or must not be performed on what objects by which roles. In addition, a rule can further prescribe the order of activities, i.e. which activities have to happen before or after other activities. The formalization of rules as Petri nets patterns has been proposed by Catt et al. And Huang and Kirchner. In contrast to Catt et al., Huang and Kirchner cannot cope with the expression of usage control policies.

Catt et al. employ Usage Control Colored Petri Nets (UCPN) for the formalization and enforcement of diverse types of obligations, i.e. actions to be performed before, during and after an activity. However, their approach assumes that the rules are integrated into the workflow, so that UCPN cannot be singled out for reuse for other workflows. Acting as a security automata, rules in Concert are captured as Petri net patterns and are not integrated into the workflow. Together with the classification of compliance requirements, this makes it

possible to organize compliance rules in categories according To their intent and semantics, thereby facilitating their formalization as Re-usable Petri net patterns or templates in other modular policy languages for usage control.

ARCHITECTURE DIAGRAM



To allow fine-grained and scalable access control for PHRs control attribute based encryption (ABE) techniques to encrypt every patient's PHR data. Different from earlier works in protected data outsourcing center on the multiple data owner scenario and separate the user in the PHR system into multiple security domains that really decreases the key managing complexity for owners and users. In this way a high degree of patient privacy is assured concurrently by developing multi-authority ABE and EC-MAABE.

CONCLUSION

The security and the privacy issues in healthcare applications is considered most imperative aspect in IoT based Body Sensor Network(BSN). Subsequently, by using lightweight anonymous authentication protocol and OCB encryption mode the confidentiality requirement is satisfied. Finally, we proposed a secure IoT based healthcare system using BSN, called BSN-Care, which can efficiently accomplish various security requirements of the BSN based healthcare system.

FUTURE WORK

To further analyze the problem of security requirement an algorithm called Attribute Based Encryption (ABE) will be used in order to accomplish a strong security. The time constrain must be taken into account in order to get a proper treatment for the patients.

REFERENCES

[1] Z. M. Bi and W. J. Zhang, "Modularity technology in manufacturing: Taxonomy and issues," Int. J. Adv. Manuf. Technol., vol. 18, no. 5,pp. 381–390, 2001.

[2] Q. Shu, Y. Hao, and D. Wang, "Integrated automatic generation of assembly sequences," J. Northeastern Univ. (Nat. Sci.), vol. 23, no. 7, pp. 652–655, 2002.

[3] Y. M. Huang and C. T. Huang, "Disassembly matrix for disassembly processes of products," Int. J. Prod. Res., vol. 40, no. 2, pp. 255–273, 2002.

[4] M. Agrawala, D. Phan, and J. Heiser, "Designing effective step-by-step assembly instructions," in ACM SIGGRAPH, San Diego, CA, USA,Jul. 27–31, 2003, pp. 828–837.

[5] Z. M. Bi, S. Y. T. Lang, W. M. Shen, and L. Wang, "Reconfigurable manufacturing systems: The state of the art," Int. J. Prod. Res., vol. 46, no. 4,pp. 967–992, 2008.

[6] G. Chryssolouris, D. Mavrikios, N. Papakostas, D. Mourtzis, G. Michalos, and K. Georgoulias, "Digital manufacturing: History, perspectives, and outlook," Proc. Inst. Mech. Eng. B: J. Eng. Manuf., vol. 223, no. 5,pp. 451–462, 2009.

[7] L. Atzori, A. Iera, and G. Morabito, "The Internet of things: A survey," Comput. Netw., vol. 54, pp. 2787–2805, 2010.

[8] Z. M. Bi, "Revisit for sustainable manufacturing," J.Sustain., vol. 3, no. 9, pp. 1323–1340, 2011

[9] T. Comes, M. Hiete, N. Wijngaards, and F. Schultmann, "Decision maps:A framework for multi-criteria decision support under severe uncertainty," Decis. Support Syst., vol. 52, pp. 108–118, 2011.

[10] L. D. Xu, “Enterprise systems: State-of-the-art and future trends,” IEEE Trans. Ind. Informat., vol. 7, no. 4, pp. 630–640, Nov. 2011.
[11] T. S. Lopez, D. C. Ranasinghe, M. Harrison, and D. McGarlane, “Adding sense to the Internet of things: An architecture framework for smart object systems,” Pers. Ubiquit. Comput., vol. 16, pp. 291–308, 2012.
[12] H. Panetto and J. Cecil, “Information systems for enterprise integration, interoperability and networking: Theory and applications,” Enterp. Inf. Syst., vol. 7, no. 1, pp. 1–6, 2013.