International Conference on Engineering & Technology (ICET-2020)

Available at: International Journal of Scientific Research and Engineering Development

RESEARCH ARTICLE OPEN ACCESS

SECURING CLOUD AIDED E-HEALTHCARE SYSTEM USING SPOC

S.VISHNUPPRIYA*, C. LAKSHMISHREE**, T. GOWSALYA**, N.DHARANIDHARAN**
* *(ASSISTANT PROFESSOR/CSE, Velalar College of Engineering and Technology, Erode*
Email: priya8.cse@gmail.com)
** *(CSE, Velalar College of Engineering and Technology, Erode*
Email: lakshmishree610@gmail.com)
** *(CSE, Velalar College of Engineering and Technology, Erode*
Email: gowsalyathangavel1908@gmail.com)
** *(CSE, Velalar College of Engineering and Technology, Erode*
Email: dharanidharannataraj@gmail.com)

ABSTRACT

The integration of wearable wireless devices and cloud computing in e-health systems has significantly improved their effectiveness and availability. This system not only reduces the costs associated to healthcare but also provides timely diagnosis to save lives. E-healthcare technology monitors the vital physiological parameters. In this paper, we propose SPOC (Secure and Privacy Preserving Opportunistic Computing) framework aims at the security and the privacy issues and develops a user centric-privacy access. Patients information will be send to the data sink by using BAN (Body Area Network). We make use of the searchable encryption technique with keyword range search and multi keyword search. Attribute Based Encryption is used to encrypt the data and store the cipher text into the data sink. Data consumer retrieves the data item from the data sink. E-Health management assists doctor and patients in easy and comfortable. The simulations on real world and synthetic data show the feasibility and efficiency of the system, and security analysis proves the privacy-preservation properties.

Keyword: wireless device, cloud computing, sensor deduction.

I. INTRODUCTION

Cloud Computing is potency in storing information, computation and maintenance value has succeeded to draw in even larger businesses yet. An individual user will connect with cloud system from his / her own devices like desktop, portable computer or mobile. Cloud computing helps tiny businesses to convert their maintenance value into profit. Tending may be a booming sector of the economy in several countries.

With its growth, come back challenges together with rising prices, inefficiencies, poor quality, and increasing quality. A larger storage during a sensing element and therefore the information collected is restricted compromised physically or nearly mentioned before by encrypting the hold on data to eliminate the data. In alphabetical listing is to replenish the info go below the surface itself to the innovative data by artful a protocol facilitate role based mostly encrypted structure. The wireless technology Health oriented network in current years of medical services. Medical treatment to the patient's prices applicable and timely enabled to medical specialists with real time health connected data. Sensor square measure used each in hospital and residential for medical purpose. They are easy, light-weight and compatible with body to control and sense. Within the Body space Networking (BAN) deal vital patient in sequence with additional alert to inevitable sensing element networks. a really difficult drawback transmitted information to secure channel branch let wireless communications. The secure information transmission is node authentication of key creation and rekeying a Body space Network preliminary trust. The coding is demanding the sole practicable possibility with the way on top of the bottom machine values considerably larger recollection to store up the info

A. SPOC

Secure and Privacy Preserving Opportunistic Computing used to achieve user-centric access control in e-healthcare emergency. SPOC framework aims at the security and privacy issues and develops communication between Doctor and patient. SPOC framework medical users can access the patient's information in secure manner. It is based on an attribute based access control. It will help the medical user to balance the high reliability PHI files. It will protect and safe guard the patient's information. When the patient information is gets exchange over the system to the Doctor may be misused and the secret key may not be secure to avoid such issues the SPOC framework is used. SPOC structure effectively protects the patient information driven get to control in E-healthcare disaster. With SPOC, smart phone resource including computing power and energy can be collected to process the PHI files during e-health care change. It will reduce the expenses to more clinical resources and detection of health condition. It performs reliability, scalability, privacy and security.

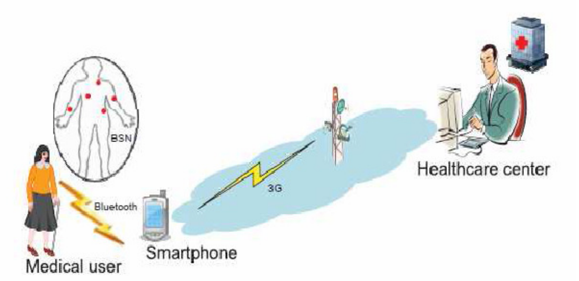

Fig. 1 Data transmission using SPOC

B. Body sensor network

Body space Network (BAN), Wireless Body space Network (WBAN) or Body sensing element Network (BSN) square measure won't to describe the applying of wearable computing devices. the most technique it covers square measure sensors, knowledge fusion and network communication. BSN system could benefit of the many differing types of sensing element to sight physiology signals, human behavior and also the encompassing surroundings. Common physiological perceived knowledge embody body motion, skin temperature, heart rate, brain and muscles activities. It's not solely new form of health care however additionally vital part of net of Things. It provides a computing hardware, code and wireless communication technology. It permits wireless communication between patient's and doctor. The device is embedded in body of patient to unceasingly monitor patients health connected data. BSN can reading a range of medical measures like pulse, vital sign and as a result letter of the alphabet knowledge are going to be generate terribly} very short amount of your time. Further, the prescriptions are going to be given by Doctor at intervals jiffy. Sensors in BNF may be many varieties in line with the varied application- specific needs to form communication sensing element uses the form because the transmission medium. BSN based mostly sensing. Element may be want to directly monitor many important signs unceasingly. The sensing element nodes have computation, storage, wireless transmission and sensing. Sensors square measure the key elements they connect the physical world. BSNs may be achieved in numerous fields like drugs, financial aid, sports and man machine interfaces. This is often special sensitive in aged individuals or patients. BANs embedded around form to watch human organs or to deliver drugs on the body. To perform each on-line and offline knowledge stream cloud computing based mostly infrastructure is aided.

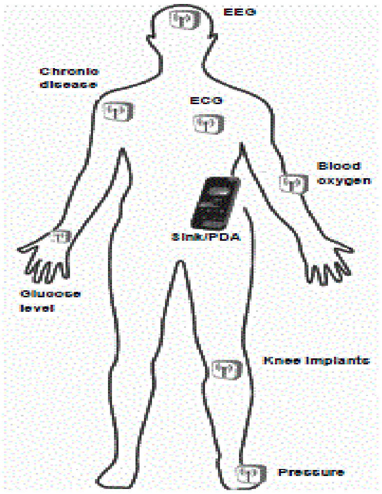

Fig. 2 Body Area Network

C. *Electro Cardio Graph(ECG) signal*

The leverage physiological signals exists research sensors to establish a session key such as Electro Cardio Graph (ECG). Secrets in sensors can pre distribute keys if necessary from the perspective of the only viable option leaves symmetric and asymmetric cryptography.

Fig. 3 Electro Cardio Graph (ECG) signal

Symmetric encryption is challenging to the key distribution involves some challenging issues and access control with symmetric encryption such as key management. The larger memory and computation power considerably store data to the limitation of memory at same time. A data sink level of protection to ensure the security protection need to have certain level captures the device of an attacker physically lost or stolen the data. The severe privacy concerns research disclosed recent many applications and read sensitive data with limited computation power. A human body is a basic scenario implanted into data securely sensor wants to distribute authorized doctors. The sensor needs expert to the privilege access its data to know in detail is no need be requested data produced a role based access control. The required property the data produced by a sensor and monitors the Electro Cardio Graph (ECG) signal.

II. EXISTING METHOD

A BAN controller device secures the transmissions with an implantable device to the patient. The mobile phone carried by this category focused in problem work in the project.

Enable secure communications within a BAN and thereby to establish secret keys from other patients and generally differs substantially in different places of the body. A unique feature of BAN its ability on leveraging research with extensive inter-pulse-intervals such as vital signs detect/measure.

Cryptographic schemes for number generator used as a unique random to all body sensors and fairly consistent patient is measurable to reading of IPI can be retrieved most existing work assumed in particular method. The patient’s health information used it to compromise adversary with UWB radar of security threat first capture the patient’s IPI information.

Electronic medical records (EMRs) on mobile addressing self-protecting and fuzzy attribute-based encryption between to securing the communications(data encryption, digital signature and access control) with focusing on via external user and an users except data controller and its external BAN with offline communications and the security of communications devices.

Healthcare provider's history treatments for illness to keep patients records using today's technology healthcare industry are not used the data. It is the fact of the concerns of an alarming rate is growing and budget healthcare amounts of the total Indians and economic problems facing Indians with healthcare is one of the top social process. The IPI information capture reliably cannot BAN devices in various places of a human body and the IPI can be measured over the area.

The neighboring nodes service to providing tasks and application of the subset by running the original application of execution to the node contributes each and opportunistically cooperating modules of a number into partitioning. The application code based on the idea of their solution especially on a single sensor node available exceeds the memory resources. Executing an application to solve the problem of storing with wireless sensor network introduce the opportunistic computing paradigm as the existing systems.

Opportunistic computing study the great interest from the research bandwidth resources used and optimizes the computational to minimize the execution time. In order and spawned on encountered nodes to derive the optimal number of replicas process between seekers and providers with service invocation model to depict the present a complete analytical model. Opportunistically contributed by invoked seekers and providers are computing as services in pervasive to abstract resources with specifically performance of service execution.

In the opportunistic computing paradigm and privacy issues exists the potential security not considered richer functionality. To provide gathered together opportunistically nodes can be available on different resources. When computing paradigm work the opportunistic for understanding important national concern for the nation's aging population to the cost of health care. Health care projected to rise to 15.9% by 2000 having doubled since 2010 to hit 70 million by 2030 to the sex over the age of 65 in existing system. The opportunistic computing paradigm existing in privacy issues and the potential security they have not considered. Different nodes can be opportunistically to provide richer functionality work gathered together the opportunistic computing paradigm with for understanding resources an available resource.

A. *Limitation Of Existing System*

The form of physical document is in the Advisor report called "Health Advisor".

The defect will be lost about and the total information is damaged in document.

Future references in the database is not stored the health information of patient.

III. PROPOSED METHOD

New secure and privacy conserving opportunist computing known as SPOC. The planned SPOC framework is employed to transfer knowledge in secure manner. The high-reliability of alphabetic character method and minimizing alphabetic character privacy square measure balanced. Patients health care data will get keep within the cloud which can be secured. Knowledge owner cipher and store the info on cloud server while not revealing the contents. Doctor and patient can have the separate login. Each doctor and patient should get registered to sign up. The communication between doctor and patient are confidential and each. Patient's physiology parameters are measured by the sensing element. Sensing element is employed to detect the pressure level, heart rate, vital sign, etc. Sensing element is embedded within or close to the body. Searchable cryptography is that the basic methodology for looking encrypted knowledge keeps within the cloud server. A new crypto logical construct known as Blind Storage. That permits a shopper to store a group of files on an overseas server and also the server doesn't learn the scale of files and also the length of the individual files. The proposed definition for satisfied searchable centric symmetric cryptography. However, their theme cannot be used for the keyword vary and multi keyword search. Considering that the info user is willing to question keyword varies or multi keyword, planned associate in nursing attribute –based multi keyword search. The Top-k observance technique to style a various multi keyword stratified search theme over encrypted cloud knowledge.

A. *Advantages*

Learner agent learns from interaction with a dynamic setting.

In these environments, providing a group of coaching knowledge for the agent is extremely troublesome or may be not possible.

Correspondingly huge number of states and actions.It provides the big numbers of users and high stream rates.

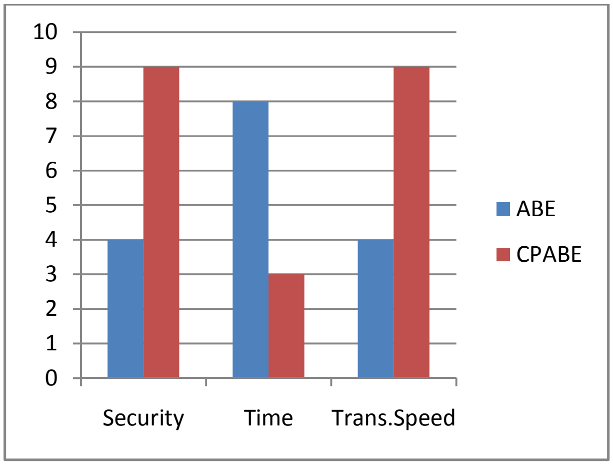

Fig. 4 The Overall comparison of Existing and Proposed Method.

IV. MODULES AND DESIGN

A. *Key Generation Center*

The KGC is employed to perform system data formatting, generate public parameters, and assign a secret key for every of the attributes a knowledge shopper claims to possess. The general public parameters ought to be put in into the sensors before they're deployed in an exceedingly BAN. A knowledge shopper ought to be able to convince the KGC that it's the owner of a group of attributes and also the KGC can generate a secret key for every attribute. One will see that the key keys square measure unambiguously generated for the info shopper, which means that random numbers have to be compelled to be related to the set of secret keys to stop collusion attacks. Sensors have all public parameters, which implies that every sensing element will construct AN access tree and encode its knowledge in line with the access tree. Once a knowledge consumer's attributes satisfy the access tree, it ought to be able to decipher the message victimization the corresponding secret keys.

B. *Sensors (Implanted and wearable Sensors):*

A BAN consists of wireless sensors known as BAN devices either embedded on/near the surface or deep-seated within the deep tissue of a personality's body. These sensors square measure exploited to observe very important body parameters or body movements, and/or management the physique by providing life support, visual/audio feedback. A BAN is often utilized by its human bearer for a range of applications, together with health care, military combat support, and preparation, simply to call a number of. Deep-seated devices suffer from very restricted resources in terms of battery power, storage, and computation capability. Wearable devices, on the opposite hand, have a lot of less tight resource constraints. They're sometimes powered and therefore the batteries are often changed comparatively simply. Wearable devices way exceed deep-seated ones in each amount and no uniformity. Example wearable devices embody the sensors watching the circulatory system the motion sensors placed on knees or in shoes, tiny cameras or video cameras hooked up to the dark glasses, and radars hooked up to the garments or the persist with assist visually-disabled persons, etc. The BAN devices ought to have sure computation capability to write in code the patient's information and store the cipher text into the information sink. Once a doctor or a nurse desires the information, she/he has to communicate with the information sink to retrieve the information.

C. Data Sink:

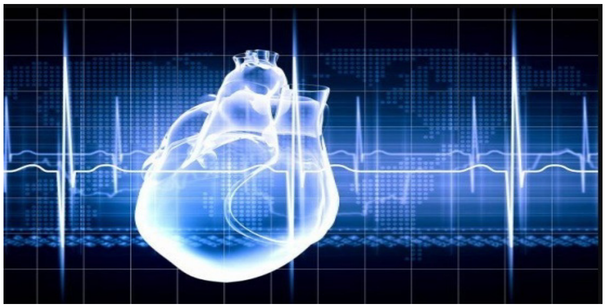

Fig. 5 Data Sink

A data sink, that may be the BAN controller or a mobile device like a Smartphone, is employed to store the patient's knowledge. We have a tendency to apply the attribute-based encoding projected by Be then court, Sashay, and Waters to code and store the cipher text within the data sink consistent with the wants of the BAN. Once knowledge customers retrieve an information item from the information sink, they will decode the information as long as they possess the key for the corresponding attributes fixed by the access tree of the information.

In a ancient framework, the information sink is employed to demonstrate the identity of an information shopper, verify its authorization standing, retrieve and code the information requested, so send the information to the information shopper. So the information sink plays a significant role and that we ought to fully trust it. In different words, if we have a tendency to use a mobile device like a smart phone with a information that permits role-based access management because the knowledge sink, we'd like to trust the smart phone to demonstrate the information shopper, check the information consumer's privilege, and establish a secure channel with the information shopper. If the good phone is physically purloined or lost, the aggressor will retrieve the information by analyzing the memory or disk. On the opposite hand, some applications in an exceeding Smartphone typically cross the road to gather needless knowledge, creating such information sink even additional prone to numerous attacks.

In our framework, we have a tendency to leverage the very fact that CP ABE will change sensors to store in cipher text; so the information sink itself has no access to the initial data. The sole demand for sink is to functionally store the encrypted data and pass around the information to the information customers that create requests. By this manner we have a tendency to minimize the trust we have a tendency to sometimes place on the information sink. so if we have a tendency to use a smart phone to store the information, the curious applications that shall learn the information will get solely the encrypted version supported the higher than analysis, during this study we have a tendency to assume that the information sink is honest however curious and straightforward to be compromised.

D. Data Consumers:

Data Consumers seek advice from the doctors and nurses or alternative specialists. To rewrite a message, knowledge shoppers ought to have the attributes that satisfy the access tree given by the information supply. once the primary time a knowledge shopper joins the system, he has to contact the KGC to get the key reminiscent of the attributes he claims to own. the keys for a knowledge shopper area unit unambiguously generated by KGC, which generally associates a random range with every key, to modify knowledge consumer's ability to rewrite a message and at the same time forestall collusion attacks.

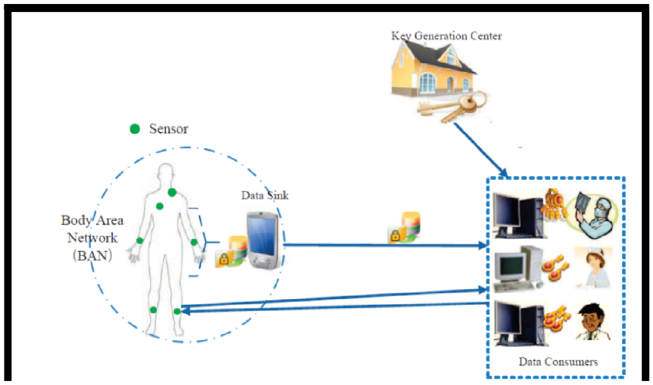

Fig. 6 System Architecture

V. CONCLUSION

In this project data is very significant more well-organized than the existing method process. In computer fields protecting information for secret message will provide better security. A number of messages depends on type of picture with message hiding occupies file is changes to certain type.

Mobile Healthcare Emergency Platform access their medical records has revolutionized the way people to store data. To secure Body Area Network additional overhead occurred earlier not only saved money to the digitization of the health information discussed many symmetric.

The hybrid key security mechanisms of Asymmetric to BAN with detail comparison approaches. Accomplish high consistency of PHI process compute to structure for medical Healthcare urgent situation. The privacy safeguard opportunistic computing projected a secure communication in urgent situation to comprehensive security investigation.

VI. FUTURE ENHANCEMENT

In future work exploit the security issues of PPSPC the internal attackers follow the protocol. The approaches with less computation and storage requirement design more practical situations in BAN. Time-consuming homomorphism encryption technique is relying studied in privacy-preserving data mining protocols to the best of knowledge. The novel non-homomorphism encryption is the most efficient one in terms. Proposed framework in m-Healthcare emergency to a custom simulator process in m-Healthcare emergency to the high-reliability of PHI process.

VII. REFERENCES

[1] J. Bettencourt, A. Sashay, and B. Waters, “Cipher text-policy attribute based encryption,” in Proceedings of the 2007 IEEE Symposium on Security and Privacy, 2007, pp. 321–334.

[2] C. Hue, F. Zhang, X. Cheng, X. Liao, and D. Chen, “Securing communications between external users and wireless body area networks,” in Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy. ACM, 2013, pp. 31–36.

[3] D. Panics, “Emerging technologies,” Engineering in Medicine and Biology Magazine, IEEE, vol. 27, no. 2, pp. 96–101, 2008.

[4] X. Liang, X. Li, Q. Shen, R. Lu, X. Lin, X. Shen, and W. Zhuang, “Exploiting prediction to enable secure and reliable routing in wireless body area networks,” in INFOCOM. IEEE, 2012, pp. 388–396.

[5] S. Ali, V. Sivaraman, and D. Ostry, “Zero reconciliation secret key generation for body-worn health monitoring devices,” in ACM Wisec. ACM, 2012, pp. 39–50.

[6] L. Shi, M. Li, S. Yu, and J. Yuan, “Bana: body area network authentication exploiting channel characteristics,” in ACM Wisec. ACM, 2012, pp. 27–38.

[7] C. Poon, Y. Zhang, and S. Bao, “A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health,” IEEE Communications Magazine, vol. 44, no. 4, pp. 73–81, 2006.

[8] K. Venkatasubramanian, A. Banerjee, and S. Gupta, “PSKA: Usable and secure key agreement scheme for body area networks,” IEEE Transactions on Information Technology in Biomedicine, vol. 14, no. 1, pp. 60–68, 2010.

[9] "EKG-based key agreement in body sensor networks," in INFOCOM Workshops 2008. IEEE, 2008, pp. 1–6.

[10] S. Cherukuri, K. Venkatasubramanian, and S. Gupta, "Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in Parallel Processing Workshops, 2003 International Conference on, 2003, pp. 432–439.

[11] K. Venkatasubramanian, A. Banerjee, and S. Gupta, "Plethysmogrambased secure inter-sensor communication in body area networks," in Military Communications Conferenc, 2008, pp. 1–7.

[12] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, and D. Chen, "OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks," in INFOCOM, 2013.

[13] J. Zhou, Z. Cao, and X. Dong, "Bdk: secure and efficient biometric based deterministic key agreement in wireless body area networks," in Proceedings of the 8th International Conference on Body Area Networks. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2013, pp. 488–494.

[14] S. Pirbhulal, H. Zhang, S. C. Mukhopadhyay, C. Li, Y. Wang, G. Li, W. Wu, and Y.-T. Zhang, "An efficient biometric-based algorithm using heart rate variability for securing body sensor networks," Sensors, vol. 15, no. 7, pp. 15 067–15 089, 2015.

[15] F. M. Bui and D. Hatzinakos, "Biometric methods for secure communications in body sensor networks: resource-efficient key management and signal-level data scrambling," EURASIP Journal on Advances in Signal Processing, vol. 2008, p. 109, 2008.

[16] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and Communications Security, 2006, pp. 89–98.

[17] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, "Body area network security: A fuzzy attribute-based signcryption scheme," to appear in IEEE Journal on Selected Areas in Communications (JSAC), Special Issue on Emerging Technologies in Communications, 2012.

[18] J. Akinyele, M. Pagano, M. Green, C. Lehmann, Z. Peterson, and A. Rubin, "Securing electronic medical records using attribute-based encryption on mobile devices," in Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices. ACM, 2011, pp. 75–86.

[19] D. Halperin, T. Heydt-Benjamin, B. Ransford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in Proceedings of the 2008 IEEE Symposium on Security and Privacy, 2008, pp. 129–142.

[20] W. Maisel, M. Moynahan, B. Zuckerman, T. Gross, O. Tovar, D. Tillman, and D. Schultz, "Pacemaker and icd generator malfunctions," JAMA: the journal of the American Medical Association, vol. 295, no. 16, pp. 1901– 1905, 2006.