International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

CONTEXT-AWARE IN PRIVACY PRESERVATION FOR HEALTH CARE SYSTEMS

R. Vengadeswari, Research Scholar, Department of Computer Science, St. Joseph's College, Tiruchirapalli, India.
P. Joseph Charles, Assistant Professor, Department of Information Technology,St. Joseph's College,Tiruchirapalli,India.
Dr.S. Britto Ramesh Kumar Assistant Professor Department of Computer Science St. Joseph's College Tiruchirapalli, India.

Abstract

Controlled transfer of information has always been a striking field of research since the data are moving around the globe. The term context-awareness denotes to the notion that computers can sense, work and react based on the environment. In recent trends, the secure transfer of data can effectively be made with the help of the context-awareness systems as it concerns with the attainment of user's activity, location and the context of users participation with the system. This paper proposes a context awareness privacy preservation system for healthcare centers with the objective of preserving user private data around and within the participants of the medical system. Two cryptographic approaches such as Advanced Encryption Standard (AES) and Message Digest 5 (MD5) are implemented to offer an end-to-end security over networks.

.

Keywords: AES, context-awareness, MD5, privacy, role.

1. Introduction

The critical issue with medical data management is the protection of private information of patients from being revealed to third parties. As the globe is interconnected, it is now possible that a patient from one location may consult a physician at a different location over the internet. The records of the patients are digitized and maintained as electronic medical records. Electronic medical records are often more useful that both patients and physicians can refer medical information wherever they are.

Transmission of electronic medical records has raised new issues on privacy as it is more prone for the attackers to hack patients' information for performing malfunctions. Information 'leakage' is seen as having the potential to discourage to both patient and physician from participating in the system. The use of encryption, secure logins and passwords are certain security measures for privacy. This paper discusses on the privacy preservation of medical data using context-awareness cryptographic techniques. The remaining section of this paper organized as follows: section 2 describes the review of literature, section 3 explains the methodology of the proposed work, section 4 contains the experimentation, section 5 elucidates the results and discussion and finally section 5 defines the conclusion and future work of propsed work.

2. Review Of Literature

Kamakshi *et al* [1] proposed a framework that allowed a systemic transformation of original data using randomized data perturbation technique and the modified data was then submitted as result of client's query through cryptographic approach. Using this approach they could achieve confidentiality at client as well as data owner sites. This model gave valid data mining results for analysis purpose but the actual or true data was not revealed.

Vasudevan *et al* [2] proposed a new solution by integrating the advantages of both privacy preserving data using role based access and cryptographic techniques with the view of minimizing information loss and privacy loss. By making use of cryptographic techniques to store sensitive data and providing access to the stored data based on an individual's role, and ensured that the data was safe from privacy breaches.

Heurix *et al* [3] provided an overview of actual privacy threats and presented a pseudonymization approach that preserved the patient's privacy and data confidentiality. It allowed (direct care) primary use of medical records by authorized health

ISSN:2319-7900

care providers and privacy preserving (non-direct care) secondary use by researchers. The solution also addressed the identifying nature of genetic data by extending the basic pseudonymization approach with query able encryption.

Kiran *et al* [4] proposed framework that performed two major tasks of secure transmission and privacy of confidential information during mining. Secure transmission was handled by using elliptic curve cryptography and data distortion for privacy preservation was ensuring by highly secure environment. The authors had used data distortion mechanism for Privacy Preserving Data Mining (PPDM) to analyze how these methods could be used in the above medical data.

Adam *et al* [5] proposed an approach for integration and querying of health care data from multiple sources in a secure and privacy preserving manner. The basic idea of their approach was to use commutative encryption to encrypt all data items in each party's data set. Commutative encryption ensured that the encrypted keys from different data sets would be equal if and only if their original values were equal. The encryption prevented any source or querying party from extracting the individually identifiable or sensitive information from the joined data set. A similar commutative decryption ensured that only the querying party could extract the final result set.

Rui et al [6] examine the privacy perceptions of both patients and clinicians/practitioners. They examine how access to the data in an EHR system should be managed and controlled. For example, a patient should be able to restrict access to her EHR if she does not want to reveal such information to family members or healthcare providers and, at the same time, the authenticity of EHR with respect to content authentication and source verifiability should be addressed. On the other hand, clinicians should apply mechanisms to obtain patients' information from multiple EHR repositories accurately, securely, and timely.

Furthermore, access to historical medical records should be, in general, granted to a practitioner if both the patient's consent and authorization from the respective Care Delivery Organization (CDO) are granted.

Giannetsos *et al* [7] distinguish privacy, integrity, and policy issues. Regarding integrity, they point out that the adversary can be both an outsider and an insider. As the personal nature of information significantly increases the interest in launching an attack (i.e. data authentication problem), such sensitive data should be delivered with the assurance that no intermediate users have tampered with them. Regarding policy, synergy between policies and technologies entails all of the challenges of interdisciplinary cooperation, the included parties should determine which issues are best addressed by policy or technology, while policy language can be used in order to express users preferences in a readable format, in case of a complex environment.

Oladimeji *et al* [8] the interchange of the EHR over ad-hoc and pervasive communication channels is susceptible to data harvesting by malicious while data can be distorted by spurious signals from a malicious attacker. It is equally important to outline which challenges a patient faces regarding health identity and anonymity. argues that If a record is so specific that not many patients match it, then releasing the data may lead to linking the anonymous HER to a patient. If a sensitive value occurs together with some Quasi Identifier attributes frequently, then sensitive information can be inferred from such attributes even though the exact record of the patient cannot be identified.

Ahamed *et al* [9] provide two indicative scenarios regarding privacy violation and information leakage in a healthcare context, from which they induce the following challenges: patient authorization is needed to acces her EHR, but only on a need-to-know basis, while (b) doctors/healthcare service providers hold the right to restrict access to prediction information, which may be kept secret for the sake of analysis and can only be revealed to the patient, upon request, after the end of treatment.

3. Methodology

This paper deals with the preservation of user private medical data through a role based access control system. The users of the system are identified as doctor, nurse and patient. The information flow of the system is controlled with the hierarchy of the role. The system is designed to reveal user's medical data only to those who are involved in the treatment process of the concern patient. Others could not view the information of one's personal data. The proposed external architecture of the privacy preserving health care data using cryptographic techniques is shown in Fig.1

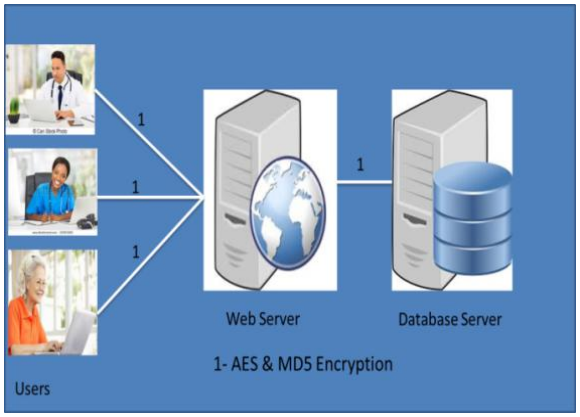

Figure 1. External Architecture of Context-Awareness Privacy Preserving Health Care Systems

Initially the users of the system are expected to register themselves before they participate in health consultation. Users role are designated as doctor, nurse and patient. The prefix of the login id is itself designed to depict the role of the user. The internal architecture of the Context-Awareness privacy preserving healthcare systems is represented in Fig 2. The internal architecture of the proposed work contains set of rules and states for every individual user according to their role. When the user comes online, both privacy manage and context manager, would respond the user with the services that they require as per the rule and state designated by them. Evaluation Engine of the context manager evaluates the user rules carefully to prevent the system from any security violations or breaches.

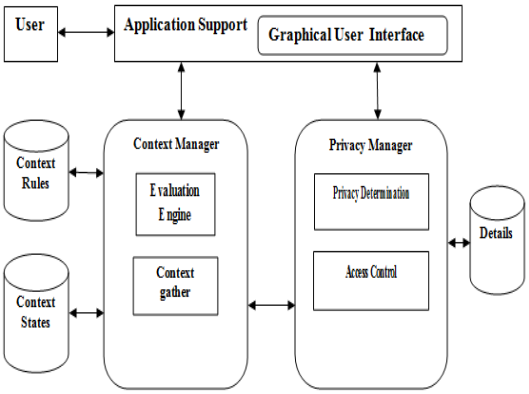

Figure 2. Context - aware privacy preservation for health care systems.

The data of proposed privacy preserving health care systems are protected using AES symmetric key and MD5 message digestion techniques. Encryption of data using AES and MD5 can protect user from several attacks such as Dos attack, man in the middle attack, insider attack, and phishing etc. AES comprises three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively.

Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys -- a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of cipher text.

AES encryption is proved to be reliable. The algorithm for AES encryption and decryption is given in Fig 1 respectively applications, and is also commonly used to verify data integrity.MD5 digests have been widely used in the software world to provide some assurance that a transferred file has arrived intact.

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic MD5 processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit words); the message is padded so that its length is divisible by 512.

```
function AES_Encrypt (M, K)
  where M = (L, R)

M ← IP(M)

    for round ← 1 to 16 do

Ki ← SK(K, round)

L  ← L xor F(R, Ki)

swap(L, R)
    end
    swap(L, R)
    M ← IP-1(M)
    return M
end
```

```
function AES_Decrypt (C, K)
where C = (L, R)

  C ← IP(C)

      for round ← 16 to 1 do

  Ki ← SK(K, round)

  L  ← L xor F(R, Ki)

  swap(L, R)
        end
    swap(L, R)
    C ← IP-1(C)
    return C
end
```

Algorithm for AES Encryption and Decryption

ISSN:2319-7900

The padding works as follows: first a single bit, 1, is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits less than a multiple of 512. The remaining bits are filled up with 64 bits representing the length of the original message, modulo 2^{64}.

Experimentation

When the user sends a login request to the web server, the client manager of the web server transfers the login screen where the credibility of the user such as user name and password are to be entered. The credentials are encrypted using AES, digested using MD5 and forwarded to the web server for authentication.

The authentication manager of the web server reverses the process of the client manager for retrieving the original data to be verified by the database manager. The data base manager verifies the user name and password by looking up the login table.

If the credentials are found to be valid it informs the client manager to throw the login page for the corresponding user or sends login failed message. Once when the authentication process is over the user may access the services that are provided to them. A doctor can prescribe medications to patients through sending messages. Likewise, a doctor may send a message to the nurse regarding diet report and observation report for the patient detail with.

Fig. 3 shows the home page of the doctor that contains services like sending or viewing incoming messages.

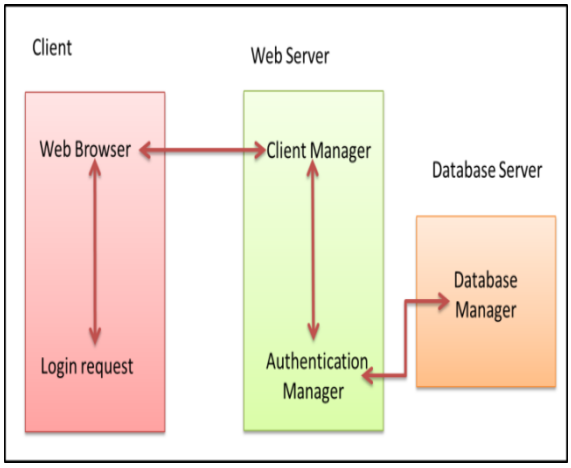

Figure 3. Information flow

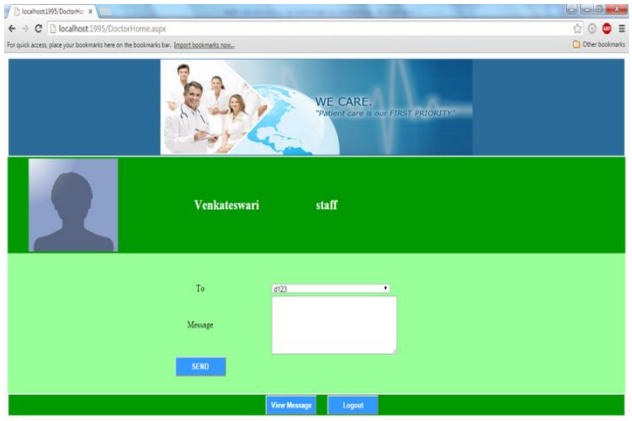

Figure 4. User Home Page

A doctor may get incoming messages from other doctors in the hospital, nurse or by the patient like a screen is represented in fig 5.

Figure 5. View Message

The encrypted data of exchange of messages as well as the personal details of the users of the system is also shown in fig.5. The data are encrypted through AES algorithm. AES works on the basis of private and public key. The server only knows the private key of the user whereas the user knows the public key of the server with which the data are encrypted and decrypted. The concept of MD5 is implied when the data is being transferred from user to server and vice versa.

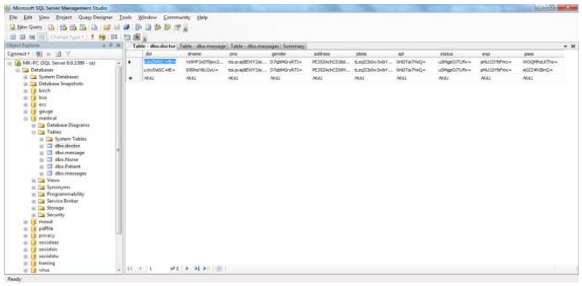

Fig. 6 Encrypted data stored in database.

ISSN:2319-7900

4. Result and Discussion

The proposed context-awareness privacy preserving health care system offers three significant features to the health centers such as confidentiality, authentication and integrity which is the most important aspects of any networking systems.

A. Confidentiality

As the messages are encrypted and sent to the recipient, it is important to ensure the confidentiality of each node. The public key encryption method uses the transmitter's public key to encrypt the messages, and the recipient uses its private key for decryption. Since each node has its own private key, only the recipient can decrypt the messages and thus the data confidentiality is ensured.

The proposed mechanism uses a P2P encryption method for message transmission. Sensor nodes use the shared secret keys with the cluster head to encrypt the messages. The cluster head uses the shared secret key with the base station to encrypt the messages. Therefore, the transmitted messages can only be decrypted with the shared keys to obtain the information. Even being eavesdropped, the attackers do not have the private key to calculate the secret key so they cannot decrypt the messages.

Even if the attackers control a node in the network, they still cannot decrypt the messages forwarded by this node. Thus, this mechanism can ensure the confidentiality of transmitted messages no matter if the network is subjected to internal or external attacks.

B. Authentication

To ensure that both the transmitter and the recipient have legitimate identities, the sensor nodes can use the cluster head's public key to ensure the certificates are generated by a legitimate node and have not been tampered with or forged during the transmission process.

C. Integrity

The message authentication code is calculated by using secret keys and the appended to the data for transmission. Therefore, the attackers cannot modify or forge the message without the secret keys. The recipient can use the authentication code to determine if the received message is legitimate, and discard the message if it has been modified. In the following, it is shown that the key management mechanism can be used for the defense against several attacks.

5. Conclusion

A healthcare environment faces several privacy threats and risks that need to be addressed due to the sensitive nature of the transmitted patient information. This work is to present the privacy requirements that need to be met in such an environment. Existing privacy research for healthcare has been reviewed, highlighting the challenges in healthcare. In this work to proposed context-aware schemes for privacy preservation in pervasive environments. An exploited a hybrid approaches to minimize user interventions in sharing context information. In the other case, there has been leveraged user behavior to automate sharing of context elements to different users. Finally, an evaluated the performance of the solutions in terms of the user experience. Simulation results have shown that our schemes are effective in reducing the number of prompts and queries, especially when interactions among different users are taken into consideration.

6. References

[1] Kamakshi, P. and Dr. Vinaya Babu, A. "Preserving Privacy and sharing the data in Distributed Environment using Cryptographic Technique on perturbed data". Journal of computing, volume 2, issues 4, April 2010, ISSN 2151-9617.

[2] Lalanthika vasudevan, S. E. Deepa sukanya, N. and Aarthi. "Privacy Preserving Data Mining using Cryptographic Role Based Access Control Approach". Proceeding of the International Multi conference of engineers and computer scientists 2008, IMECS 2008, 19-21 March 2008, Hong kong.

[3] Johannes Heurix and Thomas Neubauer, "Privacy Preserving Storage and Access of Medical Data through Pseudonymization and Encryption". Springer – Verlag Berlin Heidelberg 2011.

[4] Kiran, P. Sathish kumar, S. Dr. Kavya, N. P. "A Novel Framework using Elliptic Curve Cryptography for Extremely Secure Transmission in Distributed Privacy Preserving Data Mining". Advanced Computing: an International Journal (ACIJ), vol3, No.2, March 2012.

[5] Nabil Adam, Ph.D, Tom white M. D, Basit Shafig Ph.D, Jaideep Vaidya Ph.D, and Xiaoyun. "Privacy preserving Integration of

ISSN:2319-7900

Healthcare Data". AMIA Annu symp proc. 2007, 2007 1-5.

[6] Rui, Z. and Liu, L. "Security models and requirements for health care application clouds". Paper presented at the 33rd International Conference on Cloud Computing, USA, and July 2010.

[7] Giannetsos, T. Dimitriou, T. and Prasad, N.R. "People-centric sensing in assistive healthcare: Privacy challenges and directions". Security and Communication Networks 4.11:1295–1307.

[8] Oladimeji, E. A. Chung, L. Jung, H. T. and Kim, J. "Managing security and privacy in ubiquitous e-Health information interchange. Paper presented at the 5th International Conference on Ubiquitous Information Management and Communication, ACM, Korea, February 2011.

[9] Ahamed, S. I. Talukder, N. and Kameas A. D. "Towards Privacy Protection in Pervasive Healthcare". Paper presented at the 3rd International Conference on Intelligent Environments, Ulm, Germany, and September