# EFFICIENT EVENT DETECTION USING MACHINE LEARNING IN CLOUD COMPUTING

K. MANI
DEPARTMENT OF CSE
PAAVAI COLLEGE OF ENGINEERING
Manilavanya02@gmail.com

P. NIRMAL
DEPARTMENT OF CSE
PAAVAI COLLEGE OF ENGINEERING
Nirmalkumar2402@gmail.com

J.S. SHANMUGA
DEPARTMENT OF CSE
PAAVAI COLLEGE OF ENGINEERING
Shanmugasekaran201@gmail.com

---

## 1.ABSTRACT

Recently, the sport of mountaineering is a popular leisure activity and many people may injure while mountaineering. In the year of 2014, Chen et al. suggested a cloud-based emergency response and SOS system for mountaineering travelers when they encounter dangers. Chen et al. claimed that their proposed system is secure against various known attacks and the executive performance of the system is reasonable when the protocol is implemented on the traveler's mobile device. However, in this paper, discover that Chen et al.'s scheme is unable to protect the privacy of mountaineering travelers and the vulnerability allows a malicious attacker to spy on the electronic medical records of all mountaineering travelers by launching eavesdropping attacks. Moreover, Chen et al.'s scheme is vulnerable to off-line password guessing attack when the mobile device of the mountaineering traveler is lost or stolen by an attacker. In order to repair these shortcomings existing in Chen et al.'s scheme, based suggest an improved version of their scheme, which is provably secure in the random oracle model under the DDH and CDH problems.

## 2.INTRODUCTION

Recently, outdoor sports, such as mountaineering, river tracing, rafting, etc., have become increasingly popular. How- ever, these kinds of sports often involves considerable dangers? Since these dangers may occur in solitary roads or desert hills, a rapid and safe first aid service is vital for emergency events. Fortunately, with the ever-changing nature of wireless communication technology and the popularity of smart phones, people in danger can easily and rapidly request emergency services. In 2014, Chen et al. proposed a platform based on cloud computing architecture. In their design, a traveler who is in danger and in need of rescue and send a SOS message to a mountain emergency service center with his smart phone. An investigator or staff of this mountain emergency service center then sends this emergency message to a suitable hospital nearby. Since this traveler may come from other countries and this hospital may not have any useful information about this traveler, this hospital can send an emergency message to CSDH (Cloud Server of Department of Health), which is a cloud server storing EMR (electronic medical record) of all patients, to acquire the EMR of this traveler. With the EMR, this hospital now can arrange a proper doctor for this traveler. To the best of our understanding, this platform is the first one designed for mountaineering events.

## 3.PROPOSED SYSTEM:

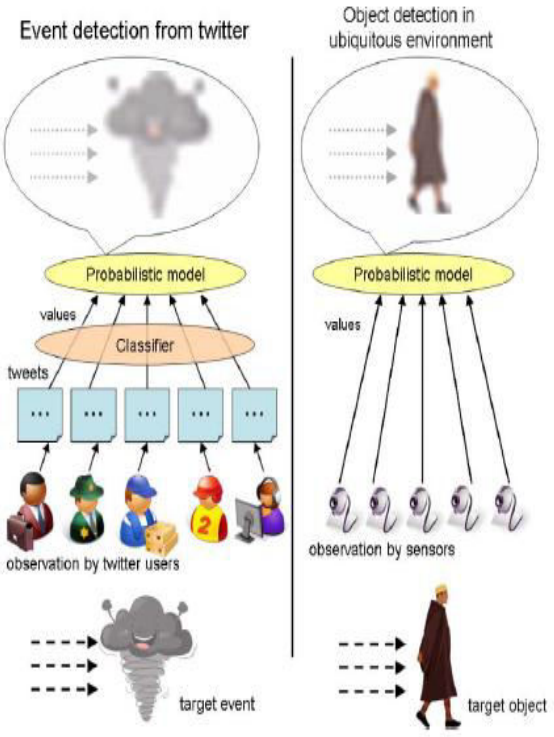
Proposed system is secure against various known attacks and the executive performance of the system is reasonable when the protocol is implemented on the traveler's mobile device. On the other hand, implement our scheme over the integers. The costs of the computation and communication consumption show that the scheme is practical in the cloud computing. Thus, could apply it to ensure the data confidentiality, the fine-grained access control and the verifiable delegation in cloud. Since policy for general circuits enables to achieve the strongest form of access control, a construction for realizing circuit cipher text-policy attribute-based hybrid encryption with verifiable delegation has been considered in our work. In such a system, the data confidentiality, the fine-grained access control and the

correctness of the delegated computing results are well guaranteed at the same time.

## ADVANTAGE

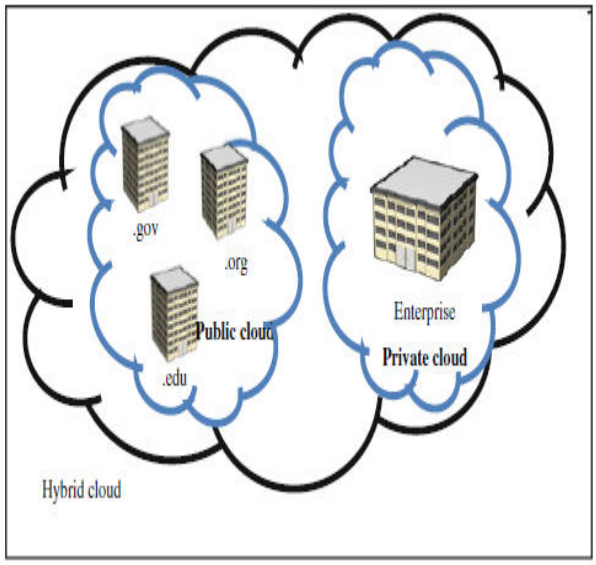
- A scheme to protect the secrecy and privacy for their platform.
- Low consumption for the cloud process.
- Data confidentiality of the process

## 4.ARCHITECTURE:




Chen et al. also proposed a scheme to protect the secrecy and privacy for their platform. They adopt the Schnorr signature, RSA, and ElGamal. However, we still found Chen et al.'s scheme has the following drawbacks and weaknesses. First, this scheme fails to protect traveler privacy. In addition, this scheme suffers from unfriendly design in registration phase. This scheme also lacks a random nonce in the delegation phase and in the signing and verification phase. Furthermore, in Chen et al.'s scheme, they claimed that a traveler does not need to worry that his mobile device will be illegally used if his mobile device is lost or stolen by attackers. However, we found that the attacker may derive the password of the traveler by launching off-line password guessing attacks.

We also try to understand the reason why this scheme is rather insecure. It appears this scheme is a common structure problem - not being proven securely in a formal model. In this paper, we first demonstrate that Chen et al.'s scheme still has some drawbacks. In order to x the drawbacks existing in their scheme, we propose a new scheme that is provable secure in the random oracle model and under the decisional Dife-Hellman (DDH) and the computational Dife-Hellman (CDH) problems. According to the performance analysis, our scheme has better efficiency compared with Chen et al's scheme.




The sport of mountaineering is becoming increasingly popular in many countries. For example, in England, according to the statistics from Sport England, roughly 147,000 people participate in mountaineering and climbing each year. Thus, we can easily conclude that mountaineering involves a significant number of people despite the potential dangers inherent in the activity. In Taiwan, about 500 people are hurt every year while mountaineering; thus, determining emergency event response techniques which use a rapid SOS service is important. As wireless technology has enjoyed giant strides in its evolution, mobile devicebased applications have become common and the computation capacity of mobile devices is rapidly increasing. Thus, we are interested in using the mobility feature of the mobile device to summon rapid aid in an emergency scenario. In this paper, we provide a platform based on cloud computing architecture and mobile devices to support an emergency response and SOS system. The cloud computing component is meant to provide an on-demand supply of computational resources, i.e., data and software, via a computer network, rather than from a local computer. That is, it is necessary to move desktop computing to a service-oriented platform which uses huge databases at data centers. The three types of cloud computing are described below and are shown in Fig. 1.

Cloud computing can increase the speed at which applications are deployed, increase innovation, lower costs, raise computational ability and increase the security via security techniques. In our proposed system, in order to respond to an SOS quickly and effectively when a dangerous situation occurs (e.g., when someone is hurt), the patient's SOS should be transmitted to the emergency service quickly in order to allow the service to immediately take action. Thus, after the emergency service receives an SOS from the patient, realizing the proxy authorization from the patient, it helps the patient notify the hospital to prepare first aid measures. As such, designing a secure and effective emergency system is our goal. Therefore, we propose a proxy signature application based on the Schnorr signature. As the Schnorr signature entails a lower computation cost and exhibits a shorter signature length than cryptography techniques RSA and ElGamal, it was adopted for use within our scheme. In an environment of emergency response and SOS systems, the fundamental characteristics are such that themessage receiver has to verify the sender's validity, and the message cannot be tampered with, eavesdropped or transmitted by an attacker. Therefore, a well-designed emergency response and SOS system should meet the following requirements:

(1). Defend against known attacks: in a public network environment, attackers are omnipresent; thus, determining a defense against known attacks has become an important issue. In our scheme, we have to defend against: tampering attacks, replay attacks, man-in-the-middle attacks, password guessing attacks, and mobile device lost attacks.

(2). Verifiability: from the proxy signature, the verifier can be convinced of the original signer's agreement by a signed message.

(3). Unforgeability: a proxy signer can create a valid proxy signature; an attacker or any unauthorized person cannot generate a proxy signature.

(4). Non-repudiation: the proxy signer cannot deny that a valid proxy signature is generated by him/her.

(5). Non-designated: when the original signer issues the certificate, he/she does not specify the identity of the proxy signer.

## 5.MODULES:

- Tweet collection
- Crawling tweets from Twitter
- Twitter Search API
- Filtering tweets using machine learning
- Semantic Analysis on Tweets
- Earthquake reporting System

## 5.1MODULES DESCRIPTION:

### 5.1.1 TWEET COLLECTION:

In this module, we develop our system by posting tweets by the users. It is necessary to collect tweets referring to an earthquake from Twitter. This process includes two steps: crawling tweets from Twitter and filtering out tweets that do not refer to the earthquake. For crawling and filtering tweets, we recommend using script programming languages.

### 5.1.2 CRAWLING TWEETS FROM TWITTER:

To collect tweets or some user information from Twitter, one must use the Twitter Application Programmers Interface (API). Twitter API is a group of commands that are necessary to extract data from Twitter. Twitter has APIs of three kinds: Search API, REST API, and Streaming API. In this section, we introduce Search API and Streaming API, which are necessary to crawl tweets from Twitter. We explain REST API later because REST API is necessary to extract location information from Twitter information. Additionally, it is known that Twitter API specifications are subject to change. When using Twitter API, it is necessary to know the latest details and requirements. They are obtainable from Twitter API documentation

### 5.1.3 TWITTER SEARCH API:

The Twitter Search API extracts tweets from Twitter, including search keywords or those fitting other retrieval conditions, in chronological order. It is possible to use language, date, location and other conditions as retrieval conditions. Some points must be considered when using Twitter Search API:

- It is possible to collect tweets posted only during the prior five days. It is not possible to search tweets posted six days ago.
- It is only possible to collect the latest 1500 tweets at one time. (Technically speaking, it is possible to access one page with a request and track pages back to the 15th page. One page includes 100 tweets at most. Therefore it is possible to acquire the latest 1500 tweets at one time.)
- One is limited to API requests.

### 5.1.4 FILTERING TWEETS USING MACHINE LEARNING:

We collected data from tweets including keywords related to earthquakes, such as earthquake, shake. Those tweets include not only tweets that users posted immediately after they felt earthquakes, but also tweets that users posted shortly after they heard earthquake news, or perhaps they misinterpreted some sense of shaking from a large truck passing nearby. When the seismic activity reached its peak, the graph of tweets invariably showed a peak. However, when the graph of tweet counts showed a peak, the seismic activity did not necessarily show a peak. Some "false-positive" peaks of the graph of tweet counts arise from mistakes by users or some news related to earthquakes. Therefore, we must filter tweets to extract those posted immediately after the earthquake. We designate tweets posted by users who felt earthquakes as positive tweets, and other tweets as negative tweets. Here, we describe the creation of a classifier to categorize crawled tweets into positive tweets and negative tweets, using Support Vector Machine: a supervised learning method.

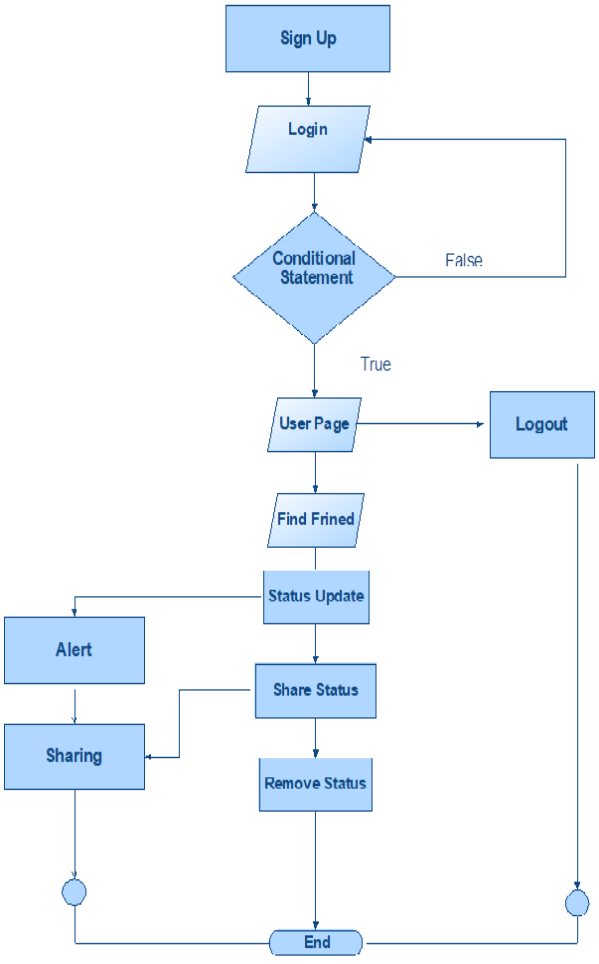
### 5.1.5 SEMANTIC ANALYSIS ON TWEETS:

Semantic Analysis on Tweet Search tweets including keywords related to a target event Example: In the case of earthquakes “shaking”, “earthquake” Classify tweets into a positive class or a negative class Example: “Earthquake right now!!” positive “Someone is shaking hands with my boss” negative Create a classifier Semantic Analysis on Tweet Create classifier for tweets use Support Vector Machine (SVM) Features (Example: I am in Japan, earthquake right now!) Statistical features (7 words, the 5th word) the number of words in a tweet message and the position of the query within a tweet Keyword features (I, am, in, Japan, earthquake, right, now) the words in a tweet Word context features (Japan, right) the words before and after the query word

### 5.1.6 EARTHQUAKE REPORTING SYSTEM:

In this module, the users will be altered if the earthquake occurs based on their location and the tweets. Effectiveness of alerts of this system Alert E-mails urges users to prepare for the earthquake if they are received by a user shortly before the earthquake actually arrives.

## 6. WORK FLOW DIAGRAM:




## 7. APPLICATION:

It is used to intimate before occur any event like environment issues (earthquake, flood, cyclone), accidental issues like (injuries).

## 8. CONCULSION:

The briefly reviewed Chen et al.'s cloud- based emergency system and shown that the process of data upload in the signing and verification phase is insecure. Although the identities of system participants are strictly verified, the attacker can still spy on the traveler's electronic medical record transmitted via public channels. In addition, Chen et al.'s scheme is also vulnerable to off-line password guessing attack in the case that the mobile device of traveler is lost or stolen. To resist these shortcomings, we put forward an improved scheme preserving traveler privacy by employing the concept of authenticated key exchange and message authentication. We have proved that our improved scheme achieves the goals of mutual authentication and key agreement in the random oracle model and the BAN logic. The analysis shows that our proposed scheme improves the security flaws of Chen et al.'s scheme while maintains the computation efficiency in cloud-based emergency system for mountaineering events.

## 9. FUTURES SCOPE:

To implement efficient event analysis and detection technique using artificial intelligent, robotics, IOT and raspberry pi.

## 10. REFERENCES:

Sport England: Primary Offer Data Information Pack for Mountaineering, accessed on Jul. 03, 2016. [Online]. Available: http://www.sportengland.org/

[2] C.-L. Chen, Y.-Y. Chen, C.-C. Lee, and C.-H. Wu, ``Design and analysis of a secure and effective emergency system for mountaineering events," Supercomputers., vol. 70, no. 1, pp. 5474, 2014.

[3] C. P. Schorr, ``Efficient signature generation by smart cards," J. Cryptal., vol. 4, no. 3, pp. 161174, 1991.

[4] B. Lee, H. Kim, and K. Kim, ``Strong proxy signature and its applications," in Proc SCIS, vol. 1. 2001, pp. 603608.

[5] R. L. Rivets, A. Shamir, and L. Adelman, ``A method for obtaining digital signatures and public-key cryptosystems," Communication. ACM, vol. 21, no. 2, pp. 120126, Feb. 1978.

[6] T. ElGamal, ``A public key cryptosystem and a signature scheme based on discrete logarithms," in Proc. Workshop Theory Appl. Cryptograph. Technical., 1984, pp. 1018.

[7] M. Bellaire and P. Roadway, ``Entity authentication and key distribution," in Proc. Annul. Int. Cryptal. Conf., 1993, pp. 232249.

[8] R. Canetti, O. Gold Reich, and S. Halevi, ``The random oracle methodology, revisited," J. ACM, vol. 51, no. 4, pp. 557594,

[9] C.-M. Chen, W. Fang, K.-H. Wang, and T.-Y. Wu, ``Comments on `An improved secure and efficient password and chaos-based two-party key agreement protocol,'" Nonlinear Dyn., vol. 87, no. 3, pp. 20732075, 2017.

[10] S. A. Chaudhry, M. S. Far ash, H. Naqvi, S. Kumari, and M. K. Khan, ``An enhanced privacy preserving remote user authentication scheme with provable security," Security. Communication Network., vol. 8, no. 18, pp. 3782 3795, 2015.

[11] C.-M. Chen, L. Xu, T.-Y. Wu, and C.-R. Li, ``On the security of a chaotic maps-based three-party authenticated key agreement protocol," J. Network. Intelligent., vol. 1, no. 2, pp. 6165, 2016.

[12] D. He, N. Kumar, and N. Chamartín, ``A secure temporal-credential- based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks," Inf. Sci., vol. 321, pp. 263277, Nov. 2015.

[13] C.-C. Lee, D.-C. Lou, C.-T. Li, and C.-W. Hsu, ``An extended chaotic- maps-based protocol with key agreement for multi server environments," Nonlinear Dyn., vol. 76, no. 1, pp. 853866, 2014.

[14] S. Kumari, S. A. Chaudhry, F. Wu, X. Li, M. S. Far ash, and M. K. Khan, ``An improved smart card-based authentication scheme for session initiation protocol," Peer-Peer Network. Appl., vol. 10, no. 1, pp. 92105, 2017.

[15] M. Burrows, M. Abadi, and R. M. Needham, ``A logic of authentication,' Proc. Roy. Soc. London A, Math., Phys. Eng. Sci., vol. 426, no. 1871, pp. 233271, 1989.

[16] K. Y. Choi, J. Y. Hwang, D. H. Lee, and I. S. Seo, ``ID-based authenticated key agreement for low-power mobile devices," in Proc. Austral. Conf. Inf. Security. Privacy, 2005, pp. 494505.

[17] T.-Y.Wu,Y.-M. Tseng, and T.-T. Tsai, ``A revocable id-based authenticated group key exchange protocol with resistant to malicious participants," Computer. Network., vol. 56, no. 12, pp. 29943006, 2012.

[18] M. Bellaire and P. Roadway, ``Random oracles are practical: Paradigm for designing efficient protocols," in Proc. 1st ACM Conf. Computer. Communication. Security., 1993, pp. 6273.

[19] C.-C. Lee, C.-T. Li, S.-T. Chiu, and Y.-M. Lai, ``A new three-party- authenticated key agreement scheme based on chaotic maps with- out password table," Nonlinear Dyn., vol. 79, no. 4, pp. 24852495, 2015.

[20] L. Zhang, S. Tang, and S. Zhu, ``A lightweight privacy preserving authenticated key agreement protocol for SIP-based VoIP," Peer-Peer Network. Appl., vol. 9, no. 1, pp. 108126, 2016.