ISSN 2277-3061

ENHANCED SECURITY MECHANISM IN CLOUD COMPUTING USING HYBRID ENCRYPTION ALGORITHM AND FRAGMENTATION: A REVIEW

Amandeep Kaur [(1)], Mr. Pawan Luthra [(2)]
[(1)] Research Scholar, Department of Computer Science & Engineering, SBSSTC, Ferozepur, Punjab.
amanthind59@gmail.com
[(2)] Assistant Professor, Department of Computer Science & Engineering, SBSSTC, Ferozepur, Punjab.
pawanluthra81@gmail.com

ABSTRACT

Cloud is a term used as a metaphor for the wide area networks (like internet) or any such large networked environment. It came partly from the cloud-like symbol used to represent the complexities of the networks in the schematic diagrams. It represents all the complexities of the network which may include everything from cables, routers, servers, data centers and all such other devices. Cloud based systems saves data off multiple organizations on shared hardware systems. Data segregation is done by encrypting data of users, but encryption is not complete solution. We can do segregate data by creating virtual partitions of data for saving and allowing user to access data in his partition only. We will be implementing cloud security aspects for data mining by implementing cloud system. After implementing cloud infrastructure for data mining for cloud system we shall be evaluating security measure for data mining in cloud. We will be fixing threats in data mining to Personal/private data in cloud systems.

Keywords

Cloud Computing, Cloud Security, Confidentiality, Security Issues, Zones, OTP, AES, RSA, Fragmentation, Replication.

Council for Innovative Research
Peer Review Research Publishing System

Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

Vol.14, No.8

www.ijctonline.com, editorijctonline@gmail.com

ISSN 2277-3061

INTRODUCTION

Cloud Computing is one of the biggest technology advancement in recent times. It has taken computing in initial to the next level. Cloud computing is one of the biggest thing in computing in recent time. Cloud computing is a broad solution that delivers IT as a service. Cloud computing uses the internet and the central remote servers to support different data and applications. It is an internet based technology. It permits the users to approach their personal files at any computer with internet access . The cloud computing flexibility is a function of the allocation of resources on authority's request. Cloud computing provides the act of uniting. Cloud computing is that emerging technology which is used for providing various computing and storage services over the Internet . In the cloud computing, the internet is viewed as a cloud. By the use of cloud computing, the capital and operational costs can be cut. Cloud computing incorporates the infrastructure, platform, and software as services. These service providers rent data center hardware and software to deliver storage and computing services through the Internet. Internet users can receive services from a cloud as if they were employing a super computer which be using cloud computing. To storing data in the cloud instead of on their own devices and it making ubiquitous data access possible. They can run their applications on much more powerful cloud computing platforms with software deployed in the cloud which mitigating the users burden of full software installation and continual upgrade on their local devices.

CLOUD TYPES

Depending on infrastructure ownership, there are four deployment models of cloud computing [6].

1) **Public Cloud**: - Public cloud [4] allows users to access the cloud publicly. It is access by interfaces using internet browsers. Users pay only for that time duration in which they use the service, i.e., pay-per-use.

2) **Private Cloud**: - A private clouds [5] operation is with in an organization's internal enterprise data center. The main advantage here is that it is very easier to manage security in public cloud. Example of private cloud in our daily life is intranet.

3) **Community Cloud**:-When cloud infrastructure construct by many organizations jointly, such cloud model is called as a community cloud. The cloud infrastructure could be hosted by a third-party provider or within one of the organizations in the community.

4) **Hybrid Cloud**: - It is a combination of public cloud [7] and private cloud. It provide more secure way to control all data and applications. It allows the party to access information over the internet. It allows the organization to serve its needs in the private cloud and if some occasional need occurs it asks the public cloud for some computing resources.

ISSUES IN CLOUD COMPUTING

• Security and privacy in the Cloud: Security is the biggest concern when it comes to cloud computing. In a cloud based infrastructure, a company gives the private data and information. This information may be sensitive or confidential. The cloud service provider helps to manage, protect and retain the information. Hence the provider's reliability is very critical. Similarly, privacy in the cloud is another huge issue. Companies and users have to trust their cloud service vendors that they will protect their data from unauthorized users. The various stories of data loss and password leakage in the media does not help to reassure some of the most concerned users.

• Dependency and vendor lock-in: One of the major disadvantages of cloud computing is the implicit dependency on the provider. The implicit dependency is known as vendor lock in. If a user wants to switch from one service provider to another then it can be very painful and cumbersome to transfer huge data from the old provider to the new one

• Technical Difficulties and Downtime: Certainly the smaller business will enjoy not having to deal with the daily technical issues and will prefer handing those to an established IT company. Hence in the cloud computing you should keep in mind that all systems might face dysfunctions from time to time. Outage and downtime is possible even to the best cloud service providers.

• Limited control and flexibility: In the cloud computing, the applications and services run on remote, third party virtual environments, companies. The users have limited control over the function and execution of the hardware and software. Hence, remote software is being used, it usually lacks the features of an application running locally.

• Increased Vulnerability: The cloud based solutions are exposed on the public internet and are thus a more vulnerable target for malicious users and hackers. On the internet nothing is completely secure. Hence people may suffer from serious attacks and security breaches. It happens due to the interdependency of the system

SECURITY CONCERNS IN CLOUD COMPUTING

In this section we first introduce some major security concern-

• **Network Availability** The value of cloud computing [2] can only be realized when our network connectivity and bandwidth meet our minimum needs: The cloud must be available whenever we need it. If it is not, then the consequences are no different than a denial-of-service situation.

• **Cloud Provider Viability** Since cloud providers are relatively new to the business, there are questions about provider viability and commitment[9]. This concern deepens when a provider requires tenants to use proprietary interfaces, thus leading to tenant lock-in.

• **Disaster Recovery and Business Continuity** Tenants and users require confidence that their operations and services will continue if the cloud provider's production environment is subject to a disaster.

• **Security Incidents** Tenants and users[3] need to be appropriately informed by the provider when an incident occurs. Tenants or users may require provider support to respond to audit or assessment findings. Also, a provider may not offer sufficient support to tenants or users for resolving investigations.

• **Transparency** When a cloud provider does not expose details of their internal policy or technology implementation, tenants or users must trust the cloud provider's security claims. Even so, tenants and users require some transparency by providers as to provider cloud security, privacy, and how incidents are managed.

• **Loss of Physical Control** Since tenants and users lose physical control over their data and applications, these results in a range of concerns:

(a) Privacy and Data With public or community clouds, data may not remain in the same system, raising multiple legal concerns.

(b) Control over Data User or organization data may be comingled in various ways with data belonging to others.

(c) A tenant administrator has limited control scope and accountability within a Public infrastructure-as-a-service (IaaS) implementation[8], and even less with a platform-as-a-service (Paas) one. Tenants need confidence that the provider will offer appropriate control, while recognizing that tenants will simply need to adapt their expectations for how much control is reasonable within these models.

(d) New Risks, New Vulnerabilities There is some concern that cloud computing brings new classes of risks and vulnerabilities. Although we can postulate various hypothetical new risks[10], actual exploits will largely be a function of a provider's implementation. Although all software, hardware, and networking equipment are subject to unearthing of new vulnerabilities, by applying layered security and well-conceived operational processes, a cloud may be protected from common types of attack even if some of its components are inherently vulnerable.

RELATED WORK

Tejinder Sharma, et.al (2013)[1]: In this paper author discuss about the cloud computing. As, the computer networks are still in their infancy, but they grow up and become sophisticated. Cloud computing is emerging as a new paradigm of large scale distributed computing. It has moved computing and data away from desktop and portable PCs, into large data centers. It has the capability to harness the power of Internet and wide area network to use resources that are available remotely.

Sonal Guleria, Dr. Sonia Vatta (2013)[2]: Describes that the Cloud computing is emerging field because of its performance, high availability, least cost and many others. In cloud computing, the data will be stored in storage provided by service providers. Cloud computing provides a computer user access to Information Technology (IT) services which contains applications, servers, data storage, without requiring an understanding of the technology. An analogy to an electricity computing grid is to be useful for cloud computing. To enabling convenient and on-demand network access to a shared pool of configurable computing resources are used for as a model of cloud computing.

Pradeep Bhosale et.al(2012)[3]: Discusses that today's world relies on cloud computing to store their public as well as some personal information which is needed by the user itself or some other persons. Cloud service is any service offered to its users by cloud. As cloud computing comes in service there are some drawbacks such as privacy of user's data, security of user data is very important aspects. In this paper author discuss about the enhancement of data security. Not only this makes researchers to make some modifications in the existing cloud structure, invent new model cloud computing and much more but also there are some extensible features of cloud computing that make him a super power.[3] To enhance the data security in cloud computing used the 3 dimensional framework and digital signature with RSA Encryption algorithm.

Jasmin James, et.al (2012)[4]: Discusses about the security in cloud computing. Cloud computing is fast growing area in computing research. With the advancement of the Cloud, many new possibilities are coming into picture, like how applications can be built and how different services can be offered to the end user through Virtualization. There are the cloud services providers who provide large scaled computing infrastructure defined on usage, and provide the infrastructure services in a very flexible manner. The virtualization forms the foundation of cloud technology where Virtualization is an emerging IT paradigm that separates computing functions and technology implementations from physical hardware. By using virtualization, users can access servers without knowing specific server details.

Cong Wang et.al (2010)[5]: In this paper, author discusses about the security in cloud computing. Cloud Computing consists the architecture of IT enterprise. The cloud computing has the many advantages in the information technology field: on demand self service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk. [5] Cloud computing brings the new and challenging security threats towards users outsourced data. For this purpose, cloud service providers are used. These are the separate administrative entities.

Ryan K. L. Ko et.al (2011)[6]: In this paper, author describes the various schemes that are used in the security of cloud computing. Cloud computing signifies a paradigm shift from owning computing systems to buying computing services. In this paper, author encourages the adoption of file centric and data centric logging mechanisms. It helps in increasing the accountability. The security in the cloud computing is a big issue. For this purpose, data transparency, access within the cloud and lack of clarity in data ownership were surfaced. Here author purpose a new scheme, which helps in providing security to cloud computing. This scheme finds out the various approaching traditional security and trust problems. Here the data centric approach is use, which helps in increasing trust and security of data in the cloud.

Shuai Han et.al (2011)[7]: In this paper, author uses a third party auditor scheme. Cloud computing technology acts as next generation architecture of IT solution. It enables the users to move their data and application software to the network which is different from traditional solutions. Cloud computing provides the various IT services, due to which it contains many security challenges. The data storage security is the big issue in cloud computing. In this paper, author purpose a new scheme called third party auditor. It helps in providing the trustful authentication to user.

Jen-Sheng Wang et.al (2011)[8]: In this paper, author about the various methods and techniques which helps in managing the security of cloud computing. The information security is critical issue in the age of Internet. The information is valuable and important. The cloud computing has made information security managing a most significant and critical issue. The information security in cloud computing requires many factors. In this paper, the Key Success Factors are used. These factors include many aspects as: external dimension, internal dimension, technology dimension, and execution dimension. These factors are used to purpose a new scheme, which is used to overcome the various problems in cloud computing that are related to the security.

Eman M.Mohamed, Hatem S.Abdelkader (2013)[9]: In this paper, author discusses about the data security issues in cloud computing. Data security model provides a single default gateway as a platform. It used to secure sensitive user data across multiple public and private cloud applications, including salesforce, Chatter without influencing functionality or performance. Default gateway plateform encrypts sensitive data automatically in a real time before sending to the cloud storage without breaking cloud application. It did not effect on user functionality and visibility. If an unauthorized person gets data from cloud storage, he only sees encrypted data. If authorized person accesses successfully in his cloud, the data is decrypted in real time for our use.

Teemu Kanstren, Sami Lehtonen, Reijo Savola(2015)[10]: In this paper, author discusses about architecture for providing increased confidence in measurements of such cloud-based deployments. The architecture is based on a set of deployed measurement probs and trusted platform modules across both the host infrastructure and guest virtual machines. The TPM are used to verofy the integrity of the probes and measurements they provide. This allows us to ensure that the system is running in the expected environment, the monitoring probes have not been tampered with and the integrity of measurement dat provided is maintained. Overall this gives us a basis for incrresed confidence in the security of running parts of our system in an external cloud-based environment.

MOTIVATION FOR RESEARCH

In present work firstly client sendsdata to server, afterwards server encrypts the data. Here AES encryption algorithm is used to encrypt or decrypt user's data file. After that encrypted data is placed on the storage cloud. At its core, the architecture consists of four components:

1). A server, then process and encrypts data before it is sent to cloud;

2). A cloud 'A' that archive another half of user's files;

3). A cloud b, that archive another half of the same user's file; and

4). A private cloud that holds the Meta data information.

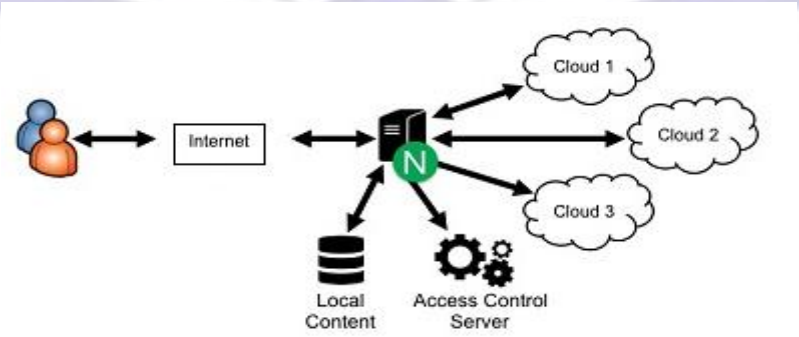

Figure 1. Client and Cloud Interaction

• Currently encrypted data is stored in different clouds.

• The cloud usage cost is very high and also complexity of the system is increased.

• This multi-cloud architecture specifies that the application data is partitioned and distributed to distinct clouds.

• The most common forms of data storage are files and database.

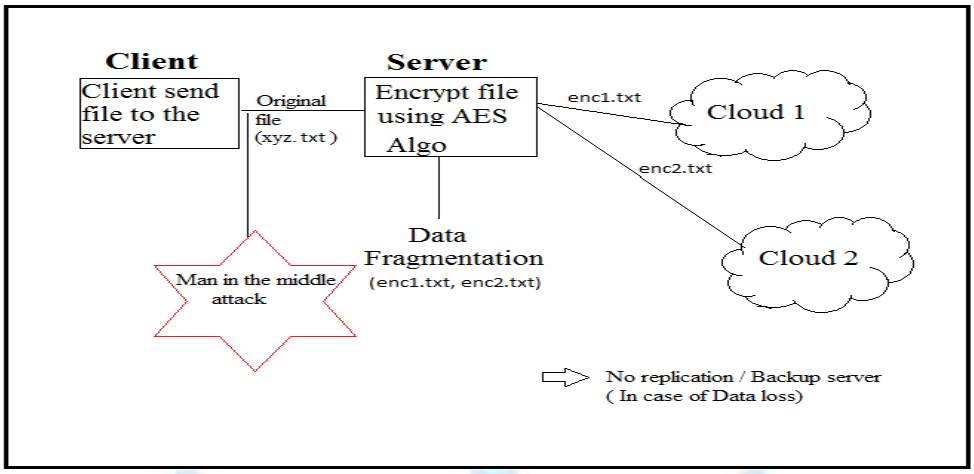

Figure 2. Problem Formulation

- Cloud based systems saves data off multiple organizations on shared hardware systems. Data segregation is done by encrypting data of users, but encryption is not complete solution. We can do segregate data by creating virtual partitions of data for saving and allowing user to access data in his partition only. Malicious activity monitoring is a tough task in cloud system as logging data might be spread over multiple hosts and data centres. Restricting user to his own virtual partition only will not allow logs to be dispersed allowing access to logs for monitoring easily. User access is another major concern in restricting user access is a major challenge in cloud based storage system. Use of virtual partition and enhanced user access control in cloud system will allow us to improve data security. Enhanced Cloud system will be compared with existing secure cloud systems. We will compare enhanced system against security, performance & ease of use.
- By distributing data on different clouds it introduces performance overhead when client needs to access all data frequently, e.g. client needs to perform a global data analysis on all data. The analysis may have to access data from multiple locations, with a degraded performance. By simply using in single cloud provider can having the following main issues: Less Security. Loss of data; No privacy; Cost of maintenance is high.

OBJECTIVES

This section states the proposed data security model in cloud computing by integrating the OTP based authentication with two encryption algorithms like AES and RSA. In the first phase, client will register and login with the cloud provider. After successful login, cloud server will generate the OTP (One Time Password).

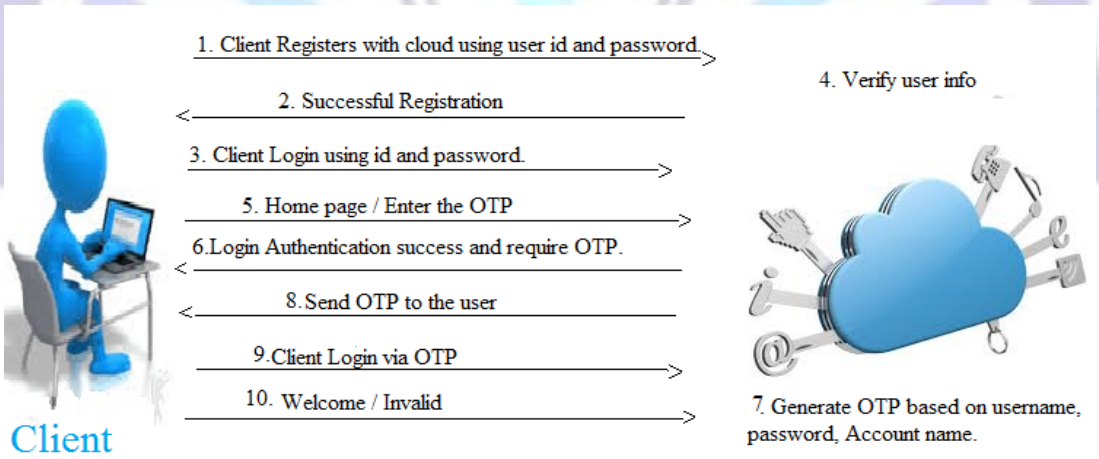

Figure 3. OTP Based Authentication Model

- Client will perform the RSA encryption before sending the data to the cloud.
- The file sent by the client is received at the server end and server will further perform the AES encryption on the received data.
- After encrypting the data, server will perform the fragmentation on the encrypted file and will send it to the cloud storage area.

- Cloud provider will receive the file and will store it in the different zones for security purposes.
- Cloud provider will also replicate the data on the backup server.

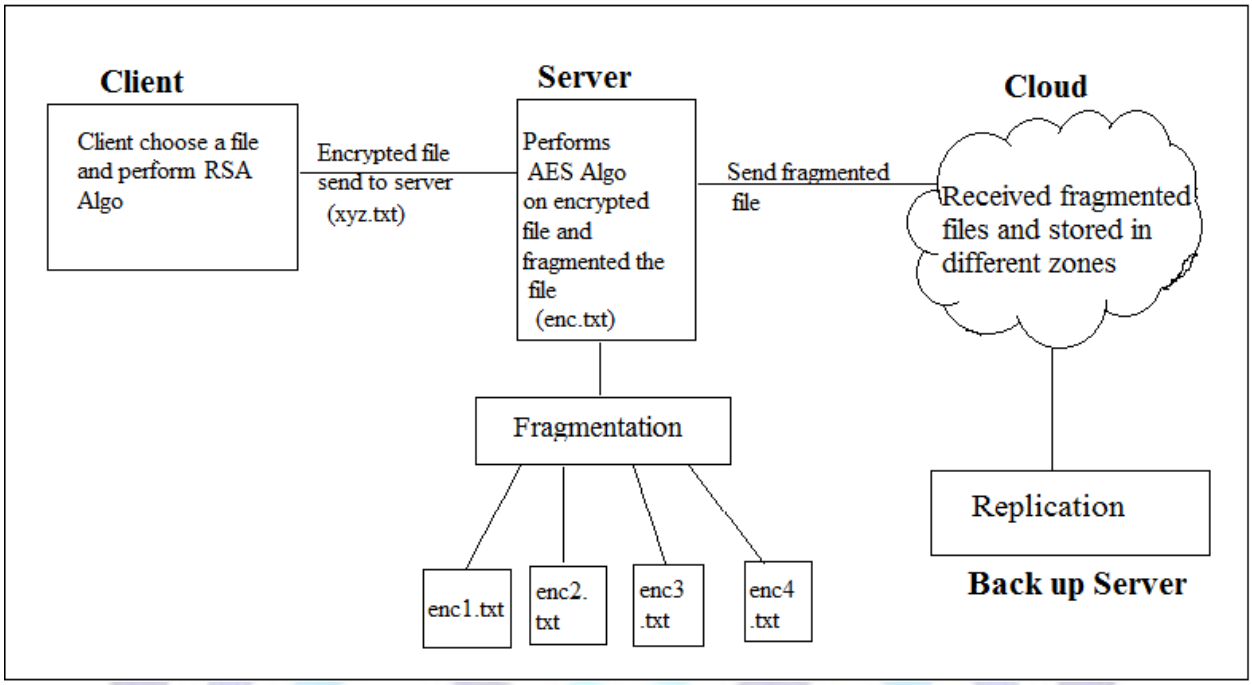

Figure 4. Proposed Cloud Security Model

We will be using the CloudSim as a simulator for implementing the proposed methodology. Cloud service providers charge users depending upon the space or service provided. In R&D, it is not always possible to have the actual cloud infrastructure for performing experiments. For any research scholar, academician or scientist, it is not feasible to hire cloud services every time and then execute their algorithms or implementations. For the purpose of research, development and testing, open source libraries are available, which give the feel of cloud services. Nowadays, in the research market, cloud simulators are widely used by research scholars and practitioners, without the need to pay any amount to a cloud service provider.

CONCLUSION

With the continuous growth and expansion of cloud computing, security has become one of the serious issues. Cloud computing platform need to provide some reliable security technology to prevent security attacks, as well as the destruction of infrastructure and services. There is no doubt that the cloud computing is the development trend in the future. Cloud computing brings us the approximately infinite computing capability, good scalability, service on-demand and so on, also challenges at security, privacy, legal issues and so on. But to solving the existing issues becomes utmost urgency. To protect against the compromise of the compliance integrity and security of their applications and data, firewall, Intrusion detection and prevention, integrity monitoring, log inspection, and malware protection. Proactive enterprises and service providers should apply this protection on their cloud infrastructure, to achieve security so that they could take advantage of cloud computing ahead of thei r competitors. These security solutions should have the intelligence to be self-defending and have the ability to provide real-time detection and prevention of known and unknown threats. To advance cloud computing, the community must take proactive measures to ensure security.

REFERENCES

[1] Tejinder Sharma, Vijay Kumar Banga. Efficient and Enhanced Algorithm in Cloud Computing, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013.

[2] Sonal Guleria1, Dr. Sonia Vatta2, to enhance multimedia security in cloud computing environment using crossbreed algorithm, Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com, Volume 2, Issue 6, June 2013.

[3] Pradeep Bhosale Priyanka Deshmukh Girish Dimbar Ashwini Deshpande , Enhancing Data Security in Cloud Computing Using 3D Framework & Digital Signature with Encryption, International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8, October – 2012.

[4] Jasmin James, Dr. Bhupendra Verma, efficient VM load balancing algorithm for a cloud computing environment, Jasmin James et al. International Journal on Computer Science and Engineering (IJCSE).

[5] Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, 978-1-4244-5837-0/10/$26.00 ©2010 IEEE.

[6] Ryan K. L. Ko, Markus Kirchberg, Bu Sung Lee , From System-centric to Data-centric Logging Accountability, Trust & Security in Cloud Computing.

[7] Shuai Han, Jianchuan Xing, ensuring data storage security through a novel third party auditor scheme in cloud computing, Proceedings of IEEE CCIS2011.

[8] Jen-Sheng Wang, Che-Hung Liu, Grace TR Lin, How to Manage Information Security in Cloud Computing.

[9] Eman M.Mohamed, Hatem S.Abdelkader, Data Security Model for Cloud Computing, 978-1-61208-245-5,ICN 2103.

[10] Teemu Kanstren, Sami Lehtonen, Reijo Savola, Architecture for high confidence cloud security monitoring, 978-4799-8218-9/15 2015 IEEE.