Journal of Theoretical and Applied Information Technology
20th January 2013. Vol. 47 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# SECURING INTERNET APPLICATIONS USING HOMOMORPHIC ENCRYPTION SCHEMES

**[1]YOUSSEF GAHI, [2]MOUHCINE GUENNOUN, [1]ZOUHAIR GUENNOUN, [2]KHALIL EL-KHATIB**

[1]Laboratoire d'Electronique et de Communications—LEC, Ecole Mohammadia d'Ingénieurs—EMI, Université Mohammed V-Agdal—UM5A. BP, Rabat, Morocco
[2]University of Ontario Institute of Technology, Oshawa, Canada

E-mail: [1]youssef.gahi@gmail.com, [2]mouhcine.guennoun@uoit.ca, [1]zouhair@emi.ac.ma, [2]khalil.el-khatib@uoit.ca

**ABSTRACT**

The trend towards delegating data processing and management to a remote party raises major concerns related to privacy violations for both end-users and service providers. These concerns have attracted the attention of the research community, and several techniques have been proposed to protect against malicious parties by providing secure communication protocols. Most of the proposed techniques, however, require the involvement of a third party, and this by itself can be viewed as another security concern. In this paper, we present a survey of different techniques that aim at secure applications, services, and routing protocols. We exhibit practical and popular systems/models and highlight the lack of privacy and confidentiality support in them. Furthermore, to avoid security breaches, we propose adopting an innovative approach that depends on data sorted, managed, and processed in encrypted form at the remote servers. To realize such an approach, the encryption cryptosystem must support both addition and multiplication over encrypted data. Finally, we highlight some novel tracks helping in the construction of a fully secure protocol based on the fully homomorphic encryption schemes.

**Keywords:** *Internet Applications, Security, Homomorphic Encryption Schemes, Cryptography, Security*

## 1. INTRODUCTION

The popularity of public networks, especially the Internet, and the unprecedented growth in their users has raised major security concerns, especially in terms of users' privacy. The risks of violating users' privacy exacerbate when we consider the growing trend towards using smart devices, the emergence of cloud services, and the interest in mobility solutions. These trends require full collaboration between clients, service providers and web hosts to form a solid foundation for a secure environment. This environment should implement sufficient security measures that can prevent intruders from performing a diverse range of malicious actions. Among the known approaches to support security are the usage of encryption/decryption techniques, key sharing, third party delegation, and blind processing. These approaches aim at hardening the communication system by combining cryptographic theory and secure computations. Having a secure communication system paves the way for a huge body of applications that require high levels of privacy preservation, like bank transactions and medical applications. In other words, taking security aspects into consideration when designing any communication system reflects into high trust in these systems, and encourages people to utilize them. However, supporting security requires paying careful attention to the following aspects:

1. **Confidentiality** and **Integrity**: Data confidentiality is an important aspect of security. It refers to that certain parties are denied access to the data unless they have passed certain authorization procedures. This authorization is often achieved based on cryptographic techniques, whereby information is actually protected by using encryption/decryption keys. However, confidentiality only guarantees that data is not accessible for unauthorized parties; another concept is needed to guarantee that the data is not altered or tampered with. This concept is called the integrity. The latter basically complements confidentiality to ensure that the accessed data is fully protected from unauthorized alterations that may cause a major breach to the accessed system.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. **Authenticity**: Authentication has an essential factor to support information security. It actually maintains and controls the access of authorized users to the services they registered for. Authentication can be realized and controlled by cryptographic keys, digital signatures, certificate authority… etc.
3. **Performance**: The time-consuming tasks of security algorithms have enticed a major interest in the research community. Although securing the different applications is a necessity, security algorithms are known to consume excessive time periods, and this leads to degradation in systems' efficiency. Hence, there should be a balance between the level of protection required and the delays that can be tolerated.

The efficiency of a protected system mainly depends on these aspects and the attention given to them at the design stage. However, since systems and applications have diverse requirements and applications, they will definitely differ in the level of security we can achieve in them.

In this work, we provide a survey of contributions that are related to the security of sensitive systems. First, we exhibit practical and popular applications and highlight the lack of privacy and confidentiality support in them. We then study different models and techniques that have been proposed to secure these applications/systems. We shed the light on the strengths and limitations of these proposals and discuss how to enhance them such that they keep pace with the rapid development in technology.

The remainder of this paper is organized as follows. In Section 2, we show main reasons of loss of privacy in Internet as well as how to provide a secure use. Then, in Section 3, we provide a survey of related works that aim at securing sensitive applications. In Sections 4 and 5, we highlight a novel track allowing development of fully secure applications based on the fully homomorphic encryption schemes. Finally, Section 5 concludes our paper and provides future research directions.

## 2. THE LOSS OF PRIVACY

In its beginning, the Internet was mainly introduced to interconnect laboratories that are committed to government research. As years passed, the main goal of using the Internet has expanded to allow billions of users to connect with one another regardless of their affiliations. Hence, nowadays, the Internet is referred to as the worldwide interconnection of people over individual networks that can be led by private parties, industries, or governments. This tremendous growth played an important role in making computer-based information systems, or even more specifically online-based systems, ubiquitous. This means that these elements are highly used in both individuals' and businesses' daily transactions. It is actually noteworthy that this technological revolution brought many advantages that can be as simple as easing the process of communication between people, or as complex as handling huge e-commerce companies' day-to-day operations. However, its drawbacks can be more harmful than individuals can ever expect. One of the most dangerous threats is the loss of online privacy.

In the digital age, Internet privacy refers to many concepts depending on people's perceptions. Some of us are more concerned about controlling their social networks, others are more anxious about the extent to which companies track their behavior whenever they browse different websites, while some people may even worry about governments monitoring their online activities. In other words, Internet privacy entails two major aspects 1) the personal information that identifies an individual such as their home address or phone number, and 2) the non-identifying information like the specific behavior of people while surfing the Internet.

### 2.1. Importance of Internet Privacy

Online privacy is actually a sensitive matter because of the increasing number of Internet users as well as the threats that menace them. It is important to be aware of the existence of a large number of hackers and stalkers that aim at violating the users' privacy and benefit from an unauthorized access to their undisclosed personal information. This unwanted behavior can, not only damage one's privacy, but also be a major source of financial and social worries. In order to be convinced why it is extremely important to safeguard Internet privacy, one should be aware of the various risks and dangers that are raised whenever an unsecure Internet access occurs.

It is common to notice that while advertising, websites target Internet users based on their interests. In order to do so, these websites should have access to their data and, sometimes, private information. Some are satisfied because they only see the advertising banners that appeal to them, however, this matter is not fully as innocent as it seems. The real issue is raised when these parties share the information they have with other entities

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

without the users' knowledge or agreement. This leads us to examine more the available Internet privacy issues that threaten people while using the Internet. Some of the privacy threats consist of the unauthorized network access, hacking, phishing, email fraud and spamming. Among these elements, hacking is the most used technique to acquire people's information and harm them. Once a party hacks users' data, they have complete control over how this information can be utilized and can misuse it for illegal or irrational purposes. Many examples can illustrate how people are exposed to Internet privacy loss, such as the case when the Internet service provider (ISP) can have full access to the users' information simply by tracking their online activities and behavior.

### 2.2. Causes of Privacy Loss

The growth of Internet along with the improvement of its different features and advantages has heightened many issues regarding online privacy of the users. Particularly, online users' fear includes the propagation of databases, the likelihood of online privacy loss and violation, as well as the misuse of the personal information that has been collected. The general causes that have contributed to the increasing of these fears involve the lack of official and legal frameworks that can play an important role into counteracting the offensive behavior of technology. Moreover, the fact that the increasing media publicity promotes the Internet usage as a flawless tool that can easily be used by people. It is rarely mentioned that different threats are awaiting the surfers of the Internet. In addition to these causes, the most dangerous one remains the fact that not all people are aware of privacy issues. Usually, people do not have the required knowledge that can protect them from falling into the trap of losing all their personal information, or worse, suffering from social and financial implications because of the different existing Internet frauds.

Currently, the approximate overall cost for the different cyber crimes is measured in billions. Even if many institutions have invested in both the development and implementation of different measures that can help improve Internet security, computer and Internet misuse is unfortunately expected to keep being a problem as years pass. The information system professionals are more anxious regarding the propagation of the unethical and unwanted behavior that may occur while making use of computers that are connected to the Internet. This fear is due to the fact that it can negatively affect both the society and the information system profession.

### 2.3. How To Deal with Online Privacy Loss

Once Internet users build a strong understanding about the dangerous online privacy issues, and are aware of the many threats that menace them, such as the fact that some websites generate their official revenues only by selling private information to other entities, they should be willing to wholeheartedly welcome protection from such threats and risks. No user would want to see their private data spread over the web and have no control over who can view the shared information. That's why online users must be vigilant whenever they are ready to surf the web.

Many perspectives can be considered while viewing Internet privacy protection measures. These perceptions range from the individual's adoption of simple behavior that allow them to control the private data that they share on the Internet and the different policies and regulations that exist, to the complex technological measures that can be acquired. Combining all these online privacy protection perceptions allows all users to be sure that their private pieces of information are successfully protected to a large degree and less likely to be compromised.

If we examine the behavior of an Internet user regarding what information he/she publishes and shares with the public over the web, we notice that the individual's control plays an extremely important role in protecting his/her privacy. A good behavior, combined with some extra cautions, contributes in effectively safeguarding any private information from malicious entities. Before they even consider sharing their private information on a website, users must be fully aware of its credibility. Within the same context, avoiding opening the links that are received from anonymous sources can spare many privacy loss or troubles because they may contain spyware that secretly collects sensitive data and automatically sends it to external, harmful people.

In order to reduce privacy loss or fraud, many policies and regulations are set to control and supervise the different usages of personal information that is submitted to a given organization, such as the companies that embed the e-commerce as part of their services. In this latter example, the users should be fully aware that some employers have access to their sensitive information while trying to ensure the service that they first requested. However, specific restrictions are set to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

specify to which degree the user's data can be used. In general, similar websites and organizations clearly state their policies and share them with users. Legal actions can be taken against any organization that does not respect the agreement or the policies about the usage of the user's private information.

Internet users must know that different technological tools were developed in order to contribute in the process of securing the user's online private data and prevent privacy loss. There is a countless number of online protection software that put together all the required packages (anti-spyware, firewalls, data encryption functionalities and setting…etc) that help the users preserve their anonymity. Making use of all of these elements allows the users to protect their sensitive information and prevent any privacy loss issues.

Nowadays, the Internet is considered as the largest information container and the most used means of communication. Promoting the social networking features, emailing and blogging have all effectively and efficiently contributed to easing, moving forward and improving the human being's life. This wonderful resource made the whole world looks like a smaller place where billions of people live. However, with the tremendous growth of the Internet, many issues were raised to harm and threaten the most sensitive information about the users: their privacy!

It is extremely important to be aware of the different dangers that can face the Internet users whenever they try to connect to the external world through a public network. One must be also aware of the different parties that present a potential fraud and should know how to deal with them. These malicious entities can be hackers, stalkers or third party users. They all aim at extracting sensitive and private data probably in order to make malicious use of it.

Finally, all Internet users must know the exact approaches that can help them secure their privacy and make use of them. As explained above, they can either make use of the policies and regulations, install the available software that secure their sensitive data, or simply control the information that they share with the public.

## 3. OVERVIEW OF SECURITY IN INTERNET APPLICATIONS

### 3.1. Database and Applications

Different security techniques have been devised for relational databases. These techniques can be organized into three categories: encryption, distribution techniques and access control modules. These techniques attempt to satisfy the requirements of database security that include the protection of privacy, data loss avoidance, and the prevention of unauthorized accesses. These requirements have been defined in [1]. In this work, the data to be protected have been split into three categories:

- **Data in use**: The data that exists in the memory of the database which is often more important than the data existing in the hard disc.
- **Data in motion**: The flow of data between both the client and the database server.
- **Data at rest**: The database stored files.

Shmueli et al. have also categorized attackers into three classes [1]: The intruders, which are external users that gain access to the database, the insiders, which belong to the system and threaten other users, and the malicious administrators, which track the system to extract private information from it. In what follows, we discuss the different security techniques proposed under the above mentioned categories.

#### 3.1.1. Encryption

Encryption is an effective approach to secure databases. With this approach, database records are encrypted and communications with the database server are made using encrypted queries. Encryption techniques have been widely adopted in the literature as a means to avoid third parties' intervention in the communications between database servers and their clients (see Figure 1). Examples of encryption techniques are provided in what follows.

Yin et al. have proposed in [2] an encryption technique based on mathematical transformation. The objective of this technique is to modify the query behavior such that clients interact with the database server in a blind fashion. In the same direction, Popa et al. have presented two mechanisms [3]. The first mechanism executes a query over encrypted data to extract the suitable records. The second mechanism is an adjustable technique that customizes encryption scheme according to each query to avoid revealing encryption possibilities.

In another context, Yan and Zhang in [4] use the homomorphic concept (which we detail in Section 4 of this paper) to propose a private homomorphic algorithm that acts on real numbers and supports the different arithmetic operations: addition,

Journal of Theoretical and Applied Information Technology
20th January 2013. Vol. 47 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

multiplication, subtraction and division. The authors have also proposed another mechanism called IOT-MW. This mechanism is responsible for encrypting/decrypting the content and monitoring queries to support communication with encrypted fields.

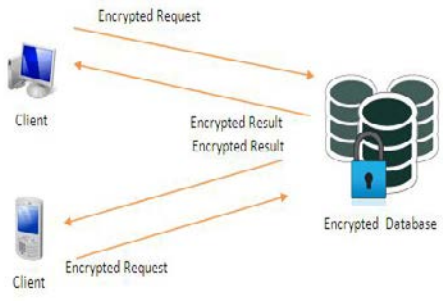


*Figure 1. Encrypted Database Architecture Without Third Parties.*

Qi-chun has tackled in [5] the problem of executing encrypted queries while considering the time consumed in encrypting the databases. The work in this paper is based on the exponential algorithm and ASCII transformation to reconstruct a new index depending on the query inputs. Then, any record of character type is converted to a larger integer before considering only four bytes of the final converted record. This is meant to achieve a significant decrease in the time needed to perform the query.

The authors in [6] and [7] have followed an approach different than the above mentioned ones. Basically, they depend on third parties to enhance the encryption efficiency. Pagano and Pagano have assumed the existence of a trusted third party that uses a re-routable deterministic encryption technique to link queries with performers [6]. The latter technique is performed without allowing both the performer and the routing module any access to the content of the queries. On the other hand, Raykova et al. have used in [7] a remote synchronizer to store the decryption keys, and maintained a database memory, instead of files stored on hard disc, as part of the proposed architecture.

It is worth mentioning that in enterprises' platforms the outsourced databases are actually utilized in a shared mode where multiple users have access to the same records. In such a context, supporting security becomes challenging and special techniques are needed to guarantee that only authorized users get access to the protected data. Yang et al. have addressed the problem of multi-user settings for encrypted databases [8]. The paper uses the bilinear maps concept to provide a private keyword search scheme that processes encrypted queries and produces encrypted results from an encrypted database. This is done without disclosing the contents of the queries or the results. The scheme manages also users revoke and denies access without need to a key renewal.

### 3.1.2. Distribution

Distributed architectures are often adopted to eliminate complex configurations, and avoid additional middleware that are expensive to repair. Distribution, in general, is realized by distributing processes among several parties and sharing tasks with different modules. This concept can be adopted to build distributed database architectures with an effective security model. Distributed databases aim at storing data in several locations and use multiple performers to manage data according to their sensitivity, see Figure 2.

The protection of privacy through employing the distribution concept has received a considerable attention in the research community. The work of Aggarwal et al. in [9] and their extensions proposed by Ganapathy et al. in [10] have presented a distributed architecture that partitions data between two un-trusted servers using a vertical fragmentation.

The system that uses encryption and some obfuscation techniques to support privacy uses a bottom up state algorithm to split queries into sub queries. The latter can be later addressed to different parties without leaving any traces. Also, the system assumes that the different servers are disconnected from each other, and the interrelated sensitive information is not saved in the same server.

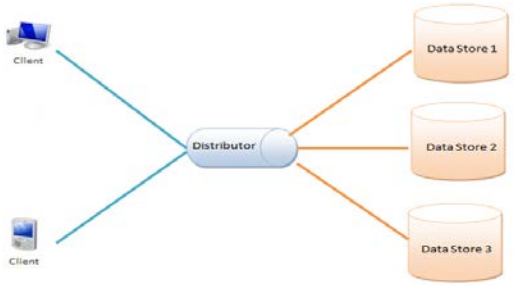


*Figure 2. Distributed Database Architecture.*

Unlike the previously described work, Yonghong has chosen the horizontal fragmentation and semantic attribute decomposition to partition

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

records over several distributed servers [11]. To preserve privacy, a probabilistic anonymity idea is employed when distributing data across servers.

On the other hand, to support the privacy using a distributed architecture and encrypted data, Al thneibat et al. in [12] decompose the topology into three components 1) the databases' clients that interact with the database system and submit queries, 2) the service provider that initiates the database structure and provides encryption keys as well as privileges to the third component, and 3) SMM module, which is an interface between the client and the databases where most of the processing is performed. This module is responsible for managing encrypted database access and processing encrypted queries according to the client's authorization.

Indeed, all presented contributions can support the privacy for database systems in different ways. However, there are some theoretical approaches that have not received sufficient attention in this area, such as the Secret Sharing Scheme (SSS). This scheme depends on distributing a secret like encryption keys or sensitive data among a group of users using SSS. This secret is then regrouped and reconstructed by combining all of the parts shared by the participants. Within the same context, Bai et al. in [13] have proposed a secure relational database management system. This system defines a parameter of access K that represents the threshold of privileges. If someone has an access to K or more databases in the distributed architecture, then they are allowed to manipulate the data. Otherwise, the access is denied.

Finally, unlike the approaches that focus on the interaction between the client and the databases, Zhang and Zhao in [14] have addressed the problem of communication between databases. The authors have considered the queries that aim at finding both the intersection and the difference between several private databases using the two-party concept where each party protects its data and do not want to reveal the content. They have also proposed to protect privacy by controlling query inputs.

### 3.1.3. Access Control

Access Control is the basic technique to protect and manage data access in a database system. This technique assigns privileges to the specific parties that can interact with the topology and then checks authentication parameters to unlock the protected data for processing. The associated architecture is often composed of three modules, the user, the database server and a control panel. The control panel verifies whether the user credentials match the control list or not, and then attributes or denies the access to the server, see Figure 3.


*Figure 3. Distributed Database Architecture*.

Database systems suffer from different types of attacks. The attacker can benefit from failures like privilege abuse, system vulnerabilities and weak audits, to gain unauthorized access to the modules and extract useful information.

These attacks can be summarized into three main categories:

a. **Brute-force**: consists of using default or weak username/passwords to gain access, along with the corresponding privileges, to the databases.

b. **SQL Injection**: refers to submitting bad SQL queries into systems to change the behavior of the database and trace its responses.

c. **Privilege escalation**: aims at granting good privileges to a legitimate such that he/she is provided with more authorities than he/she should have.

To face these attacks and protect the privacy, a number of contributions have been proposed. Burtescu has presented four axes to deal with these attacks [15]. It advises to ignore the queries that require heavy processing of sensitive records. Then, it suggests hiding the exact value of the returned result, replacing it by an approximate one, and adding fake results in order to confuse the attacker in case its request requires only one answer. Yangqing et al. in [16] have combined an audit module with a rights control mechanism based on the twice login technique to trace requests' behavior and manage access to the database. Furthermore, Ruzhi et al. in [17] have adopted a third party concept to provide security in the database system. They suggest using a Gateway mechanism that manages all entrances including the database admin. This new module includes four components

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

to ensure an efficient system management. The first component is an authentication model that presents access rules. The second component is a transparent proxy module that protects database configurations. The third component is an attack protection module that detects and prevents different attack techniques. Finally, the fourth component is a connection monitoring module that controls the communication flow between the database and the users. Li et al. in [18] have addressed control access for encrypted databases. They propose a mechanism to authenticate queries for encrypted databases and return encrypted results. Also, they advise to accompany each encrypted result with a proof that helps to reconstruct the result using a chained hashing technique. The authors in [19, 20] have considered the special case of web databases access. Ahmad et al. in [20] have considered the multi level access control in web databases and categorized control access into three classes: mandatory, discretionary and role based access controls; whereas Bouchahda et al have proposed to manage control access based on the application profiles concept [19]. The latter defines and manages a set of SQL queries with specific permission levels varying for one session to another. This approach allows an adjustable control for many profiles.

### 3.2. Secure Remote Execution

Remote execution is a trend by which users, with limited hardware capabilities, can benefit from the powerful resources of a remote server, see Figure 4. This can be realized using the cloud computing concept, which provides users with a set of resources and services over the Internet. Cloud computing allows users to upload their binaries and interact with the result; as if these operations were executed locally.

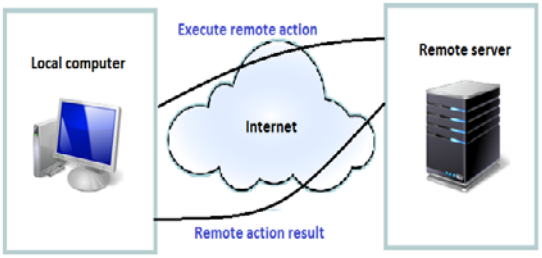


*Figure 4. Remote Execution.*

However, from the client side, these operations are actually performed on unknown and un-trusted servers. On the other hand, from the server side, the uploaded binaries are not verified, all the time, and may cause real threat. Therefore, several security concerns rise in this context, like having users susceptible to tracking. This necessitates the need to secure the remote execution operation, and the importance of protecting servers from malicious and unknown users. In order to reach these goals, many approaches have been proposed and we organize them into three main categories:

a. **Access control policies**: Program restriction policies are efficient mechanisms that provide servers with the ability to protect themselves against programs at execution. These mechanisms provide some controls that define whether a program is authorized to run. This is besides a set of different execution rules that manage the access process. These rules are useful in identifying the software using some information exported with it such as, the hash information, the certificate authority and the program's zone. The hash information is a cryptographic signature that identifies the software using its associated hash value, the file length and the hash ID. The certificate authority identifies the software publisher, and therefore, helps in making the software trustworthy. The certificate defines a code signing information that points to the owner of that certificate. Finally, the programs' zone refers to the location from where it was uploaded. A number of research studies have focused on enhancing software execution policies such as [21]-[26]. In [21], Pandey et al. have provided a general access control policy by defining a declarative access constraint language to restrict access to system components. In [22], Kiriansky et al. have proposed a number of requirements that support security at program execution. At first, access program is restricted depending on its origin. Then, limits are imposed to control access based on the source and the destination as well as the transfer type. Finally, a program is forced to pass through different checkpoints that ensure its trustworthiness. In [23], Song et al. have used a logging mechanism that provides access only to allowed components. They have also proposed an architecture that utilizes a key repository, a mandatory access control, and encryption to form an efficient access control method. Abbasi et al. in [24] have focused mainly on web applications, and therefore, have proposed the use of secure web proxies and an extensible access control markup language based on authorization policies. This work has also proposed to secure the communication between the web server and the protected web pages by means of the asynchronous communication protocol. Kim and Kim have

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

introduced a different approach that makes use of virtualization concepts to divide the execution environment into two disconnected domains with different security policies [25]. One domain is dedicated for service requests. It transforms consumer requests into an understandable message, using a multiplexer. Then, the message is submitted to the second domain, which acts as a service provider. Finally, Alves et al. in [26] have improved a runtime platform by modifying the TLS connection to implement a transport component for secure session execution.

b. **Obfuscation**: The obfuscation technique helps in protecting programs against tracking and monitoring as they run remotely. This method is used to transform the source code into another equivalent, but irreversible, form that is difficult to understand. Obfuscation focuses on the protection of the data structure and the control flow of the code. While, the first consists of hiding the source code formatting and the attributes' name, the second consists of obfuscating the control flow of the program that includes program statements, jumps, returns…etc. These controls are modified by either replacing call methods by their body or fake instructions and useless code that sets blind the program behavior. A set of contributions, namely [27]-[33], where the authors have addressed programs' obfuscation and have proposed different models to make it hard to reverse engineer these programs. Toyofuku et al. in [27] have proposed the use of random values to hide the control flow of a program. In the proposed technique, an index is assigned to each method and then, during the execution, a random value is generated to decide which method to invoke. This technique makes it hard to follow the execution and protects the program from static analysis. The work in [28] makes understanding the program hard by firstly inserting additional statements, and then replacing jumps, method calls and returns by a set of fake instructions that lead to the obfuscated operation. The contribution of [30] is different than the previous ones as it has focused on dynamic analysis. The authors have proposed a mechanism based on diversification concept to disallow running the programs several times and logging their traces. In [31], the authors have proposed the use of fake variables and simple loops that add a huge number of possible execution paths. Armoogum and Caully in [32] have suggested three obfuscation techniques: A variable renaming procedure, a comment removal mechanism, and a control statement insertion that consists of adding useless statements (like if statement, loops, dead code…etc) to confuse the disassembling. In [33], Wei has provided an additional obfuscation technique that consists of transforming functions into a table function that only shows the input and the output data. Finally, Chen et al. in [29] have proposed a binary obfuscation technique based on the taint tags and the opaque predicates.

c. **Cryptography**: Encryption has often been used to protect sensitive data in several areas against malicious and unauthorized users. It consists of employing and managing a set of encryption/decryption keys that lock/unlock a specific piece of data. The same concept has also been used to encrypt some software modules in order to obfuscate their behavior and secure the whole architecture. The contributions [34], [23], [24], [35], [33], and [36] are key examples of such architectures. In [34], Patel et al. have proposed an architecture where the program information are encrypted using a secure key and stored in a dedicated processor. Whereas the authors of [23], [24] and [35] have chosen encryption techniques that aim at protecting web page contents, data and software by storing decryption keys and allowing only authorized users to access their content. In the same direction, the work presented in [33] has advocated the use of RSA encryption and the impossibility of factorization of prime numbers to control the computational complexity. On the other hand, Brenner et al. have discussed in [36] a different concept and have focused on computations over encrypted data using HES. This work has proposed a scheme that designs encrypted circuits using an integer representation, and allows a performer to operate over them without being aware of their content.

### 3.3. Location Based Services and Mobility Solutions

In the recent decades we have noticed that both the growth of the smart phone industry and the rise of connectivity have resulted in the emergence of a diverse set of products and services. These products and services have paved the way for the development of new promising business models. Among these technologies, Location-Based Services (LBSs) have attracted the utmost attention in the research community. In general, we shall

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

mention that these services rely on the development of wireless networks, the innovation of positioning services, and the availability of information. These three elements are mainly used to determine the current position of a user, and therefore, locate the closest businesses or services (banks, restaurants, universities…etc) around that user. The user can enquire about that information by communicating wirelessly with an LBS server. However, since this technology deals with sensitive information (like the current position of the user and his/her daily habits), providing a secure architecture that allows the above mentioned elements to interact anonymously between each other becomes an essential task. Therefore, several approaches have been devised to resolve this problem. These approaches provide various secure models for the LBS technology, and aim at protecting the privacy of the querier and the location whereabouts. The contributions that aim at protecting the querier's information and hiding their real identity tend to prevent LBS servers from collecting information to identify the users. T""he approaches that we are referring to employ anonymity techniques such as [37]-[41] or pseudonym like [42] and [43]. They all aim at obfuscating the real use and mislead the service providers. The anonymity techniques work on protecting user identity from its neighbors precisely. This means that when a client enquires about a specific location, the anonymizer module replaces the query by a box that combines the user location with those of its neighbors, and sends it instead of the query that was originally requested. The anonymizer then distributes the generated response to the appropriate user while making use of the real identity. Within the same principle, pseudonym is another technique by which users protect their identity. This technique uses fake identifiers instead of the real ones and delegates the mapping between them to a location intermediary. Jorns et al. in [42] have designed a system architecture for using safety LBS while relying on pseudonym transaction. The latter consists of generating unique pseudonyms for each transaction such that no fake identifier can be reused again within subsequent operations. Using a different approach, the work presented in [43] relies on random numbers and strings to generate strong pseudonyms that are used as a basis for an LBS authentication mechanism.

Within the same context of enforcing the privacy and security of the user's location, several techniques have been developed. The main concepts that have been utilized in these techniques are relying on K neighbors, sending a cloaking region instead of the true location, and initiating several fake requests. The first technique, which is K-anonymity, depends on hiding the location information among the K-1 surrounding locations. Then, instead of working with the real location, the combination of all neighbors' locations is employed (see [44], [45], [40], and [41]). This concept has been extended to provide another technique called the cloaked region. This technique was first proposed by [46]. It depends on using the dimension of a particular region, the size of which depends on the specified security level, and protecting the location privacy by sending requests to the whole region instead of one location. On the other hand, Kido et al. [47] and You et al. [48] have proposed a different method to reach the same goal. Their technique relies on a third party component that adds to the original request many fake queries, with different fake identities, to prevent LBS from revealing the true information. Furthermore, Argadna et al. [49] have proposed an obfuscation technique that transforms the location measurements by changing both the radius and the center, and then sends the obfuscated location to LBS. Wightman et al. in [50] have focused on three pre-existing techniques: the randomization, K-anonymity and clocking region, and then proposed new extensions. Basically, the authors have introduced three techniques: N-Rand, N-Mix and N-Dispersion. While the randomization technique consists of changing the center of an area by another random point to allow users obfuscate their real location, the N-Rand enhances this concept by introducing another parameter that defines the suitable distance of obfuscation. The N-Mix technique relies on randomly generated locations instead of adopting the basic concept of K-anonymous, which relies on pre existing users' location. Finally, the N-Dispersion technique enhances the concept of dispersion, which consists of de-centering the circular area, by performing n trials while still looking for the new displacement. A different but simple technique has been introduced by He et al. in [51]. It works on cheating on the sent location by modifying the GPS API and sending fake locations instead. The authors in [52] have relied on K-anonymity to define different cells in order to hide the path a user follows from source to destination, whereas the contribution of Pingley et al. has developed query perturbation-based scheme that relies on generating several fake queries that take into account the query context [53]. Finally, Chen and J. Pang have proposed in [54] a different scheme that relies on some metrics

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

to design the most secure region for a specific user profile.

### 3.4. Ad-Hoc Wireless Networks

Ad-hoc wireless networking is the revolutionary approach that allows all the devices that belong to the same communication range, and support the necessary wireless equipment, to directly exchange information in a peer-to-peer mode. These devices, called nodes, join and leave the network dynamically and collaborate in a benevolent manner by forwarding packets to other neighboring nodes. However, many challenges arise against the efficiency of the ad hoc network's architecture because of the nodes' availability problem, and the fact that this technology does not rely on pre-existing topologies. The latter factor has received a special attention in the literature, especially that is has a direct impact on routing protocols. In general, the routing concept relies on the voluntary cooperation of various nodes that are able to forward packets from a given source to a specific destination. Given the importance of routing in the network, guaranteeing a secured topology is essential to preserve the privacy. This is because malicious and selfish nodes, if available, may mislead nodes' collaboration and make packet delivery probabilistic. In order to avoid this problem and ensure a secure exchange of information, several mechanisms have been proposed. The most common mechanism in this context is the trust-based methodology. This mechanism enforces the fact that each node evaluates its neighbors and assigns them trust values that are continuously updated based on their degree of cooperation. Hence, trust values are used to define a trust route. Within the same context, Gera et al. in [55] have based their work on an effective combination of both a trust value approach and a multipath route technique. From one side, the trust value approach depends on collaborations with only faithful nodes. On the other side, the multipath route technique chooses several paths to reach the destination and forwards the packet over them in order to increase the delivery rate. Parvin et al. in [56] have proposed the use of a given threshold to decide whether to collaborate with a specific node or not. Basically, the proposal uses different parameters, like the requesting information, the type of data, and the exchange history, to calculate a value that is associated with each node. If a node's associated value is greater than the set threshold, then it is allowed to be part of the routing process. El-Bendary et al. in [57] has focused on the direct diffusion routing algorithm that mainly relies on sending low frequency requests and acts according to the feedback (positive or negative). This algorithm has enabled the authors to design an authenticated acknowledgment-based protocol. This protocol inherits many features from this technique, like the propagation phase and the authentication stage that validates the ACK message, this latter is used to confirm the delivery. On the other hand B-Tebibel in [58] has proposed to protect the routing protocol using a hashed, one-time passwords protocol that consists of checking each hop while constructing the path. Within the same context and using a different approach, the technique that has been presented in [59] depends on an identity-based routing protocol that uses digital signatures to ensure that the collaborating nodes are credible. This protocol also checks the remaining energy in each of these nodes to confirm their readiness to participate in the route. Similarly, the contributions in [60] and [61] have used the energy levels as well as the past behavior of the nodes to decide which path is more secure. The authors in [62] have used a different approach that relies on the information from the application layer to design a cross-layer approach, which monitors the network and put away the packets from the danger zone, and a routing protocol. This approach consists of broadcasting a route discovery action by sending a probe message, and then locates the area where malicious nodes exist in order to successfully route the packets away from them. Finally, Abumansoor and Boukerche in [63] have proposed to use the node's location information, mobility, and stability to decide whether it can be trusted as part of the route or not.

### 3.5. Video On-Demand Services

In the recent decades, the growth of Internet infrastructure and the improvement of various streaming protocols have resulted in the emergence of a wide portfolio of interesting services. Among these services, Video On-Demand (VOD) has attracted the utmost attention. VOD enables users to retrieve and have full access of a large set of videos at their convenience, and this has contributed to the widespread popularity of VOD. However, this useful service faces major security challenges, especially related to the confidentiality of service providers and the privacy of end users. Service providers seek to protect their own video store by granting access only for authorized clients. On the other side, clients require that service providers do not monitor or track the different services they purchase. In order to achieve these levels of protection, several secure protocols have been proposed and studied. Most of the suggested protocols have adopted encryption techniques that

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

obfuscate videos content and enforce a secure transfer.

Lee et al. have used the digital watermarking technique to protect video content and trace illegal distribution [64]. This technique primarily encrypts the video, by applying different XOR operations, and then transmits it to the appropriate destination which is encrypted using a suitable key as well. From the client's perspective, the video is watermarked using the appropriate user ID in order to deny any illegal distribution. The work presented in [65] has proposed a different approach that makes use of both compression and joint encryption to protect the video content. This means that the encryption scheme enforces the use of two different encryption keys instead of one. The first key, named the temporal key, is used to encrypt every single frame in the video. The first temporal key, associated to the first frame, is generated from the video key created by the video provider. Every other temporal key is hashed from its previous one associated to the previous frame. Because every frame is divided into several slices, the scheme makes use of a second key, called the spacial key, to encrypt each slice. This powerful technique aims at protecting the system from any frame loss incidents. The authors in [66] have combined a hierarchical encryption strategy with XOR operations to provide a secure encryption scheme for the video content, and allow only authorized nodes to decrypt the data. The work in [67] has relied on Galois filed polynomials to provide a robust encryption algorithm. This algorithm encrypts the intra frame by using secret sharing techniques and provides safe entities with the requested access. To achieve the same goal of encrypting the video content, Yeung et al. have used in [68] the 8x8 block technique, while the authors in [69]-[71] have chosen partially encryption techniques to increase the performance of their systems. On one hand, Dubois et al. have relied on a selective encryption technique that partially encrypts the content of the video [69]. Their approach firstly analyzes each macro block separately, using some metrics and measures, and then decides whether it will be encrypted or not without interfering with the level of security. On the other hand, the work in [70] has relied on the expected quality, the available information about the content, and the multimedia scene to make excessive use of the Huffman code compression and partially encrypt the video content. Similarly, Swaminathan and Mitra have partially encrypted in [71] the video contents based on the entropy and the sensibility of the samples. Due to the importance of the privacy issue, Varalakshmi et al. have come up in [72] with a different approach that combines both the permutation code algorithm and dynamic keys in order to successfully protect confidential video transmission. In this approach, the permutation table is calculated by means of DCT coefficient and video motion measures.

It is undeniable that the security of Internet applications, services, and routing protocols can be achieved by employing different techniques. However, the most common approach followed by researchers is to adopt a third party concept, which is considered a major hole in the architecture because it may be a single point of attack. As a result, a system that ensures a direct secure communications between all parties can be more successful, and therefore, we advocate the use of HES as they are well aligned with this need.

## 4. ALETRNATIVE APPROACH: HOMOMORPHIC ENCRYPTION SCHEMES

Homomorphic encryption allows performers to compute correct operations over encrypted values without being aware of their content. This possibility is due to the fact that the encryption circuit is defined as a group homomorphism, which preserves operations in the group. Group homomorphism makes the computing over encrypted or plain values of the same effect. This flexibility resolves security issues in a variety of applications that delegate sensitive processing to un-trusted third parties.

In this section, we overview the history of homomorphic encryption and describe its mechanisms and characteristics. We also highlight different applications where the involvement of HES is beneficial.

### 4.1. History

The existence of an efficient homomorphic encryption has been standing an open question for a long time. The first model has been proposed in 1978 by Rivest, Adleman, and Dertouzos [73]. They have used the exponentiation and large integers to design an additive and multiplicative homomorphic circuits called the RSA. RSA uses fact that it is difficult to factor large prime numbers to define a strong public key cryptosystem. This key is used to encrypt data and perform simple operations over them. Many other works (like [74]-[78]) have followed the same concept in order to provide more efficient homomorphic schemes. The GM scheme [74] proposed by Goldwasser and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Micali is a probabilistic asymmetric public key encryption system that produces a ciphertext of size bigger than its associated input plaintext and then performs additions modulo 2 over that ciphertext. ElGamal in [75] has used the Diffie-Hellman key exchange concept to define another probabilistic asymmetric key encryption algorithm based on exponentiations. Following these attempts, Paillier has proposed in [76] the first secure and efficient additive scheme; it relies on operations in the ring of integers modulo $P^2$ where P is the product of two large primes. Thereafter, this interesting scheme has been the subject of other extensions (see [78] and [77]) that aimed at generalizing its basic concept. These extensions have used either the context of elliptic curves or computing in the rings of integers modulo $P^{s+1}$, where Paillier's scheme is the case with s = 1. Despite the obvious progress achieved in performing computations over encrypted values, the cited schemes are considered only semi-homomorphic since they support either additions or multiplications, but not both operations at the same time. Therefore, providing a scheme that supports both additions and multiplications has remained an open challenge until 2005, when Boneh et al. published their scheme in [79]. Although the latter could only support a single multiplication and many additions, it has paved the way for other attempts to provide robust schemes, such as the FHE that has been introduced by Gentry [80].

### 4.2. The Somewhat Homomorphic Encryption Schemes

The first FHE scheme that has been proposed by Gentry [80] was a form of encryption that supports performing arbitrary additions and multiplications, at the same time, on encrypted values. It uses the polynomial form $c = pk * q + 2 * r + m$ to define a probabilistic public key cryptosystem, where m is the bit value to encrypt as c, r and q are two random integers, and pk is the public key with the requirement that 2*r is smaller than pk /2. Then, the decryption is correctly retrieved by carrying out two modulo operations such that $m = c \bmod sk \bmod 2$, where sk is the correspondent secret key. In more details, the proposed scheme consists of four main modules:

a. **KeyGen (λ)**: This module outputs two random values pk and sk, which are the public and secret keys, respectively. These outputs are based on the parameter of security λ that specifies the length of encryption keys and the encrypted value.

b. **Encrypt (pk, m)**: This module encrypts (transforms) a bit value {0, 1} into a big integer at the order of $\lambda^7$-bit number that has the same parity as the original bit value.

c. **Decrypt (sk, c)**: This module decrypts the input ciphertext c based on the appropriate secret key sk .

d. **Evaluate (pk,C, *)**: This module presents the ciphertext result of the performed circuit C over the encrypted values.

The goal of this scheme, which is called a Somewhat Homomorphic Encryption Scheme (SHES), is to provide conditioned number of operations over protected data. This condition relies mainly on the fact that the ciphertext c mod pk (called the noise of the scheme) should be smaller that pk/2. However, this noise value, which doubles after each addition and squares after each multiplication, exceeds the threshold pk/2 after a finite number of operations, and the correct decryption will not be guaranteed anymore. Therefore, Gentry has proposed a bootstrapping procedure to remove the noise and provide augmented number of algebraic computations.

### 4.3. Bootstrapping and the Fully Homomorphic Encryption Schemes

The key idea behind bootstrapping is to re-encrypt a bounded ciphertext to refresh its noise value and then support more computations. The bootstrapping encrypts a fired ciphertext c into a new ciphertext $c^+$, which is a double encryption of the plaintext, with a fresh noise. Furthermore, all homomorphic properties are applied on that new ciphertext, which is an encrypted form of the old one. Thereafter, after many computations and before the encrypted result exceeds the threshold, one can perfectly decrypt tat result to retrieve another ciphertext that has the same parity as the plaintext.

The bootstrapping technique uses a public key to re-encrypt every bit in the ciphertext and produce a new clean ciphertext with smaller noise. Then, it uses an encrypted private key to remove the inner layer of the encryption and extract the original ciphertext. It is apparent that the original plaintext is simply a double decryption of the bootstrapped values.

By adopting a bootstrapping technique, The SHES produces a FHES that supports unlimited number of both additions and multiplications. It is worth mentioning, however, that bootstrapping is a time consuming task since re-encryption is usually performed over big integer values.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

## 5. TOWARD FULLY SECURE INTERNET APPLICATIONS

Homomorphic encryption is an efficient technique to enhance the security measures of un-trusted systems/applications that stores and manipulates sensitive data. This strong protection of data results from the capability, allowed through HES, to accept encrypted inputs and then perform blind processing to satisfy the user query without being aware of its content, whereby the retrieved encrypted data can only be decrypted by the user who initiates the request. Thus, this allows clients to rely on the services offered by remote applications without risking their privacy, even though the integrity of these servers may be questionable.

Database systems and Remote execution can both rely on HES concept to execute queries over encrypted data for either searching in an encrypted database or performing operations in an un-trusted powerful server. The inputs could be encrypted by the client and sent to the server for a blind processing. The latter performs the requested operation and returns an encrypted result to the client. The advantage of this system is that the remote server knows neither the content nor the position of the records affected by the query.

Location-Based Services can also rely on the HES technique to provide strong protection for users' information. HES makes possible to the LBS retrieving location-related information and find the suitable target without being aware of the user's position or the point of interests he/she is requesting.

Existing security models for Routing Protocols, especially trust-based technique, can also benefit from HES to provide additional security layers. In a trust-based protocol, each node can perform its trust circuit and then communicate, to its neighbors, the resulting trust evaluation in an encrypted format. This way, nodes can effectively protect their privacy.

Video On-demand Services can also based on HES to conceive a private platform, where users can purchase videos from networks with low security measures. This idea is to encrypt users' queries and blindly (that is, without being aware of their contents) process/execute them. This way, the service provider cannot be aware of the user selection.

## 6. CONCLUSION

In this paper we have highlighted a number of techniques that aim at securing applications, services, and routing protocols. However, we have seen that most of these techniques still suffer from the leak of security and need to be enhanced. Therefore, we have discussed the importance of HES and how they can protect the privacy of users and secure exposed applications. In our future work, we will use HES to propose novel models with efficient architectures for some sensitive applications.

## REFRENCES:

[1] E. Shmueli, R. Vaisenberg, Y. Elovici, and C. Glezer, "Database encryption: an overview of contemporary challenges and design considerations," In *Proceedings of SIGMOD*, pp. 29-34, 2010.

[2] C. Yin; R. Sun, and S. Xue, "A Modified Query Algorithm for Private Data Security Facing E-commerce,"In *Proceeding of Circuits, Communications and Systems*, Pacific-Asia, pp. 585-587, 2009.

[3] R. A. Popa, Catherine M. S. Redfield, N. Zeldovich,, and H. Balakrishnan, "CryptDB: protecting confidentiality with encrypted query processing," In *Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles*, pp. 85-100, 2011.

[4] H. Yan and X. Zhang, "Design of an extended privacy homomorphism algorithm," In *the 2nd IEEE International Conference on Emergency Management and Management Sciences*, pp.834-837, 2011.

[5] H. Qi-chun, "Research on ciphertext index method for relational database," In *the 2nd IEEE International Conference on Computer Science and Information Technology*, pp. 445-449, 2009.

[6] F. Pagano and D. Pagano, "Using in-memory encrypted databases on the cloud," *In the 1st International Workshop on Securing Services on the Cloud*, pp.30-37, 2011.

[7] M. Raykova, A. Cui, B. Lui, B. Vo, T. Malkin, S. Bellovin, and S. Stolfo, "Usable Secure Private Search," In *IEEE Security and Privacy, IEEE computer Society Digital Library*, pp.1-15, 2011.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[8] Y. Yang, H. Lu, and J. Weng, "Multi-User Private Keyword Search for Cloud Computing," In *the Third International Conference on Cloud Computing Technology and Science*, pp.264-271, 2011.

[9] G. Aggarwal, M. Bawa, P. Ganesan, H. Garcia-Molina, K. Kenthapadi, R. Motwani, U. Srivastava, D. Thomas, Y. Xu, "Two Can Keep a Secret: A Distributed Architecture for Secure Database Services," In *Proceedings of the 2nd Biennial Conference on Innovative Data Systems Research*, pp. 186-199, 2005.

[10] V. Ganapathy, D. Thomas, T. Feder, H. Garcia-Molina, and R. Motwani, "Distributing data for secure database services," In *Proceedings of the 4th International Workshop on Privacy and Anonymity in the Information Society*, pp.1-10, 2011.

[11] Y. Yonghong, "Privacy Protection in Secure Database Service," *In the Second International Conference on Networks Security Wireless Communications and Trusted Computing*, pp. 218-222, 2010.

[12] Ahmed M.A. Al thneibat, Bahaa Eldin M. Hasan, and Abd El-Fatah .A. Hegazy, "Secure Outsourced Database Architecture,"In *International Journal of Computer Science and Network Security*, Vol.10 No.5, pp. 246-255, 2010.

[13] L. Bai, S. Biswas, and F. Ferrese, "Design of a Reliable Distributed Secure Database System," In *Proceedings of the Fifth International Conference on Networking, Architecture and Storage*, pp. 91-99, 2010.

[14] N. Zhang and W. Zhao, "Privacy Protection Against Malicious Adversaries in Distributed Information Sharing Systems,"In *IEEE Transactions on Knowledge and Data Engineering*, Vol.20, No.8, pp.1028-1033, 2008.

[15] E. Burtescu, "Database security attacks and control methods," In *Journal of applied quantitative methods*, Vol. 4, No. 4, pp. 449-454, 2008.

[16] Z. Yangqing, Y. Hui, L. Hua, and Z. Lianming, "Design of a New Web Database Security Model," In *the Second International Symposium on Electronic Commerce and Security*, pp.292-295, 2009.

[17] X. Ruzhi, G. Jian, and D. Liwu, "A database security gateway to the detection of SQL attacks," In *the 3rd International Conference on Advanced Computer Theory and Engineering*, pp. 537-540, 2010.

[18] F. Li, M. Hadjieleftheriou, G. Kollios, and L. Reyzin, "Authenticated Index Structures for Aggregation Queries," In *ACM Transactions on Information and System Security*, Vol. 13, No. 4, pp. 1-35, 2010.

[19] A. Bouchahda, Nhan Le Thanh; A. Bouhoula, F. Labbene, "Enforcing Access Control to Web Databases," In *the 10th International Conference on Computer and Information Technology*, pp.612-619, 2010.

[20] K. Ahmad, J. Shekhar, S. Sharma, and K.P. Yadav, "A coalesce model for secure database," In *the 3rd International Conference on Electronics Computer Technology*, pp.373-376, 2011.

[21] R. Pandey, B. Hashii, M. Lal, "Secure execution of mobile programs," In *Proceedings of Information Survivability Conference and Exposition*, pp.362-376, 2000.

[22] V. Kiriansky, D. Bruening, and S.P. Amarasinghe, "Secure Execution via Program Shepherding," In *Proceedings of the 11th USENIX Security Symposium*, pp. 191-206, 2002.

[23] Z. Song, J. Molina, and C. Strong, "Trusted Anonymous Execution: A Model to Raise Trust in Cloud," In *the 9th International Conference on Grid and Cooperative Computing*, pp.133-138, 2010.

[24] A.G. Abbasi, S. Muftic, I. Hotamov, "Web Contents Protection, Secure Execution and Authorized Distribution," In *the Fifth International Multi-Conference on Computing in the Global Information Technology*, pp.157-162, 2010.

[25] Y.-H. Kim, J.-N. Kim, "Building Secure Execution Environment for Mobile Platform," In *the First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering*, pp.119-122, 2011.

[26] N. Alves, R. Hu, N. Yoshida, and P.-M Deni "Secure Execution of Distributed Session Programs," In *Proceedings of the Third Workshop on Programming Language*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

*Approaches to Concurrency and communication-cEntric Software*, pp.1-11, 2010.

[27] T. Toyofuku, T. Tabata, and K. Sakurai, "Program obfuscation scheme using random number to complicate control flow," In *EUC Workshops, LNCS* 3823, pp. 916–925. 2005.

[28] I.V. Popov, S.K. Debray, and G.R. Andrews, "Binary obfuscation using signals," In *Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium*, pp. 1-16, 2007.

[29] H. Chen, L. Yuan, X. Wu, B. Zang, B. Huang, and P.-C. Yew, "Control flow obfuscation with information flow tracking," In *the 42nd Annual IEEE/ACM International Symposium on Micro architecture*, pp. 391-400, 2009.

[30] S. Schrittwieser and S. Katzenbeisser, "Code obfuscation against static and dynamic reverse engineering," In *Proceedings of the 13th international conference on Information hiding*, pp. 270-284, 2011.

[31] Z. Wang, J. Ming, C. Jia, and D. Gao, "Linear obfuscation to combat symbolic execution," In *Proceedings of the 16th European conference on Research in computer security*, pp. 210-226, 2011.

[32] S. Armoogum, and A. Caully, "Obfuscation Techniques for Mobile Agent code confidentiality" In *Journal of Information and Systems Management*, Vol. 1, No. 1, pp. 25-36, 2011.

[33] Y.Y. Wei, "Two obfuscation methods by controlling calculation amounts and by table function for watermark," In *the International Journal of Computer Science and Applications*, Vol. 8, No. 1, pp. 110-122, 2011.

[34] K. Patel, S. Parameswaran, and S.L. Shee, "Ensuring secure program execution in multiprocessor embedded systems: A case study," *In the 5th IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis*, pp.57-62, 2007.

[35] J. Biskup, B. Carminati, E. Ferrari, F. Muller, and S. Wortmann, "Towards Secure Execution Orders for CompositeWeb Services," In *the IEEE International Conference on Web Services*, pp.489-496, 2007.

[36] M. Brenner, J. Wiebelitz, G. von Voigt, and M. Smith, "Secret program execution in the cloud applying homomorphic encryption," In *Proceedings of the 5th IEEE International Conference on Digital Ecosystems and Technologies Conference*, pp.114-119, 2011.

[37] T. Xu and Y. Cai, "Location Anonymity in Continuous Location-based Services," In *ACM GIS'07*, pp. 300–307, 2007.

[38] T. Xu and Y. Cai, "Exploring Historical Location Data for Anonymity Preservation in Location-based Services," In *IEEE Infocom'08*, pp. 547–555, 2008.

[39] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-based Services through Spatial and Temporal Cloaking," In *Proceedings of the 1st international conference on Mobile systems, applications and services*, pp. 31–42, 2003.

[40] B. Gedik and L. Liu, "A Customizable k-Anonymity Model for Protecting Location Privacy" In *IEEE International Conference on Distributed Computing Systems*, pp. 620–629, 2005.

[41] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The New Casper: Query Processing for Location Services without Compromising Privacy," In *Proceedings of the 32nd International Conference on Very Large Data Bases (VLDB'06)*, pp. 763–774, 2006.

[42] O. Jorns, G. Quirchmayr, and O. Jung," A Privacy Enhancing Mechanism based on Pseudonyms for Identity Protection in Location-Based Services," In *the Australian Computer Society*, Vol. 68, pp. 133-142, 2007.

[43] J. Zeiss, and O. Jorns, "Context-Based Privacy Protection for Location-Based Mobile Services using Pseudonyms," In *the Ninth International Conference on Mobile Data Management Workshops*, pp. 81-87, 2008.

[44] D. Reid, "An Algorithm for Tracking Multiple Targets," In *IEEE Transactions on Automatic Control*, Vol. 24, No. 6, pp. 843–854, 1979.

[45] B. Gedik and L. Liu. A Customizable k-Anonymity Model for Protecting Location Privacy," *Technical report, Georgia Institute of Technology*, 2004.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[46] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preserving Anonymity in Location Based Services," In *Technical Report TRB6/06, Department of Computer Science,National University of Singapore*, 2006.

[47] H. Kido, Y. Yanagisawa, and T. Satoh, "An Anonymous Communication Technique using Dummies for Location-based Services," In *IEEE ICPS'05*, pp. 88–97, 2005.

[48] T. You, W. Peng, and W. Lee, "Protect Moving Trajectories with Dummies," In *Proc. Int'l Workshop Privacy-Aware Location-Based Mobile Services*, 2007.

[49] C.A. Ardagna, M. Cremonini, S. De Capitani di Vimercati, and P. Samarati, "An Obfuscation-Based Approach for Protecting Location Privacy," In *IEEE Transactions on Dependable and Secure Computing*, Vol. 8, No. 1, pp. 13-27, 2011.

[50] P. Wightman, W. Coronell, D. Jabba, M. Jimeno, and M. Labrador, "Evaluation of Location Obfuscation techniques for privacy in location based information systems," In *the 2011 IEEE Latin-American Conference on Communications (LATINCOM)*, pp.1-6, 2011.

[51] W. He, X. Liu; and M. Ren, "Location Cheating: A Security Challenge to Location-Based Social Network Services," In *the 31st International Conference on Distributed Computing Systems*, pp.740-749, 2011.

[52] G. Ji, Y. Sun, and X. Ma, "Path planning for privacy preserving in location based service," In *the 15th International Conference on Computer Supported Cooperative Work in Design*, pp.162-167, 2011.

[53] A. Pingley, Z. Nan, F. Fu, C. Hyeong-Ah, S. Subramaniam, and Z. Wei "Protection of query privacy for continuous location based services," In *Proceedings of INFOCOM*, pp.1710-1718, 2011.

[54] X. Chen and J. Pang, "Measuring Query Privacy in Location-Based Services," In *Proceedings of CODASPY 2012*, pp. 49-60, 2012.

[55] P. Gera, K. Garg, and M. Misra, "Trust based multi-path routing for end to end secure data delivery in manets," In *Proceedings of the 3rd International Conference on Security of Information and Networks*, pp. 81-89, 2010.

[56] S. Parvin, S. Han, B. Tian, and F.K. Hussain, "Trust-Based Authentication for Secure Communication in Cognitive Radio Networks," *In the 8th International Conference on Embedded and Ubiquitous Computing*, pp.589-596, 2010.

[57] N. El-Bendary, O.S. Soliman, N.I. Ghali, A.E. Hassanien, V. Palade, H. Liu, "A secure directed diffusion routing protocol for wireless sensor networks," In *the 2nd International Conference on Next Generation Information Technology*, pp.149-152, 2011.

[58] T. Bouabana-Tebibel, "A Secure Routing Scheme for DSR," In *the First International Symposium on Software and Network Engineering*, pp.95-100,2011.

[59] W. Li, H. Li; M. Xie, and S. Bu, "An Identity-based Secure Routing Protocol in WSNs," In *the Seventh International Conference on Computational Intelligence and Security*, pp.703-706, 2011.

[60] M.E Mahmoud, and X. Shen, "Trust-Based and Energy-Aware Incentive Routing Protocol for Multi-Hop Wireless Networks," In *the IEEE International Conference on Communications*, pp.1-5, 2011.

[61] G. Zhan, W. Shi, and J. Deng, "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs," In *IEEE Transactions on Dependable and Secure Computing*, Vol.9, No.2, pp.184-197, 2012.

[62] M.R. Faghani, and Uyen Trang Nguyen, "Incident-driven routing in wireless sensor networks, a cross-layer approach," In *the 7th International Conference on Collaborative Computing: Networking, Applications and Work sharing* , pp. 402-406, 2011.

[63] O. Abumansoor, and A. Boukerche , "Towards a Secure Trust Model for Vehicular Ad Hoc Networks Services," In *Proceedings of the IEEE conference on Global Telecommunications (GLOBECOM 2011)*, pp.1-5, 2011.

[64] M.-H. Lee, V. So, and J. Zhao, "A key-code watermarking algorithm for video content protection," In *2010 IEEE International Conference on Wireless Communications, Networking and Information Security*, pp.702-706, 2010.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[65] S.D. Roy, Jun Tian; H. Yu, and Wenjun Zeng, "A multi-layer key stream based approach for joint encryption and compression of H.264 video," In *2011 IEEE International Conference on Multimedia and Expo*, pp.1-6, 2011.

[66] Q. Li, Y. Shen, and L. Li, "A visual information encryption algorithm for video conference," In *2010 IEEE International Conference on Information Theory and Information Security*, pp.305-308, 2010.

[67] L.M. Varalakshmi, G.F. Sudha, and V. Vijayalakshmi, "Enhanced Encryption schemes of video for real time applications," In *2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies*, pp.408-413, 2011.

[68] S.-K. A. Yeung, S. Zhu, and B. Zeng, "Perceptual video encryption using multiple 8×8 transforms in H.264 and MPEG-4," In *2011 IEEE International Conference on Acoustics, Speech and Signal Processing*, pp.2436-2439, 2011.

[69] L. Dubois, W. Puech, and J. Blanc-Talon, "Smart selective encryption of CAVLC for H.264/AVC video," In *2011 IEEE International Workshop on Information Forensics and Security*, pp.1-6, 2011.

[70] S.T.F. Al-Janabi, K.S Rijab, and A.M. Sagheer, "Video Encryption Based on Special Huffman Coding and Rabbit Stream Cipher," In *Proceedings of Developments in E-systems Engineering*, pp.413-418, 2011.

[71] V. Swaminathan, and S. Mitra, "A partial encryption scheme for AVC video," In *2012 IEEE International Conference on Emerging Signal Processing Applications*, pp.1-4, 2012.

[72] L.M. Varalakshmi, V. Bharathi, V. Sudha, and V.Florence, "A selective encryption scheme for H.264 video based on permutation code and dynamic keys," In *2012 International Conference on Computer Communication and Informatics (ICCCI)*, pp.1-5, 2012.

[73] R. Rivest, L. Adleman, and M. Dertouzos, "On data banks and privacy homomorphisms," In *Foundations of Secure Computation, Academic Press*, pp. 169–177, 1978.

[74] S. Goldwasser and S. Micali, "Probabilistic encryption and how to play mental poker keeping secret all partial information," In *Proceedings of the fourteenth annual ACM symposium on Theory of computing*, pp. 365-377, 1982.

[75] T. El-Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," In *CRYPTO*, pp. 10-18, 1984.

[76] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," In *EUROCRYPT*, pp. 223-238, 1999.

[77] I. Damgard and M. Jurik, "A generalisation, a simplification and some applications of paillier's probabilistic public-key system," In *Public Key Cryptography*, pp. 119–136, 2001.

[78] S. Galbraith, "Elliptic curve paillier schemes," In *Journal of Cryptology*, Vol. 15, No. 2, pp. 129–138, 2002.

[79] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," In *Theory of Cryptography TCC'05*, pp. 325-341, 2005.

[80] C. Gentry, "A fully homomorphic encryption scheme," *PhD thesis, Stanford University*, 2009.