ENABLING EFFICIENT, SECURE AND PRIVACY PRESERVING MOBILE CLOUD STORAGE

K.PRADEEP[1]
Assistant Professor
Dept of Computer Science & Engineering
RVS College of Engineering & Technology,
Coimbatore
muthupradeep22@gmail.com

K.MADHAVAN[2]
712819104017
Dept of Computer Science & Engineering
RVS College of Engineering & Technology,
Coimbatore

A.JEROLD CHRISTOPHER[3]
712819104715
Dept of Computer Science & Engineering
RVS College of Engineering & Technology,
Coimbatore

P.HEMALATHA[4]
712819104725
Dept of Computer Science & Engineering
RVS College of Engineering & Technology,
Coimbatore

***Abstract*—Clients can get a handy cloud storage solution thanks to mobile cloud storage (MCS). In this article, we provide a productive, safe, and privacy-preserving mobile cloud storage system that concurrently safeguards data confidentiality and privacy, particularly the access pattern. In particular, we provide an OSU protocol as the fundamental building block of the suggested mobile cloud storage system. The client can obliviously retrieve an encrypted data item from the cloud and update it with a new value by generating a small encrypted vector using OSU, which is based on onion additively Secure encryption with constant encryption layers. This greatly reduces the client's computation and communication overheads. Our work is particularly advantageous for MCS scenarios because to its fine-grained data structure, light client-side processing, and constant connection overhead. Also, by using the file chunks method, our system may be tested for its resistance to malicious cloud. With our improvement, we split a file into pieces and replicate the broken data among cloud nodes. Each server keeps a portion of a data file, ensuring that even in the event of a successful attack, the attacker would not learn any useful information.**

Keywords—Fall Detection, Machine Learning, Classifiers, Activities of Daily Living, Gait analysis, Monitoring, Health system

I. INTRODUCTION

In mobile cloud storage (MCS), data is stored on a cloud and can be accessed from anywhere with mobile devices. Due to the attractive properties, MCS is becoming more and more popular. Some large companies provide MCS services for business purposes, i.e. Apple iCloud, Dropbox,Microsoft OneDrive and Google Drive.In many situations, the cloud is not considered fully trusted. Thus, the client may employ encryption schemes to keep data confidential before uploading it to the cloud. However, in MSC-based applications, data always be re- lated to certain information, such as location information in location based services. In this situation, which item of data is being accessed leaks addition information to the cloud server. By utilizing this leaked information of access pattern, the cloud may infer the operation of the client and even the content of the encrypted data. For example, in a searchable encryption system, a cloud can identify approximately 80% of the search queries by applying a general inference attack with access pattern leakage and minimal background knowledge [1]. Oblivious technology, such as oblivious transfer (OT) [2], oblivious storage (OS)3] and oblivious random access machine (ORAM) [4], is a kind of technology that can protect both data and access pattern. Generally speaking, these technologies allow a client to access its outsourced data stored in an untrusted cloud without revealing which items have been visited or even what kinds of operations are requested. Due to the high- level privacy preservation, these technologies have been widely applied in various application scenarios such as searchable encryption [5]–[7], encrypted hidden volumes [8], [9], cloud storage [10]–[13], multi-party computation [14]–[18], etc. However, there are some challenges to employ existing oblivious schemes into MCS scenario due to several reasons. Firstly, mobile devices are generally connected to the Inter- net via wireless networks, such as ad-hoc, LTE, and Wi-Fi. That means the mobile devices have limited communication bandwidth to download and upload data. Thus, some schemes suffered by the well-known communication band- width overhead lower bound result O(log N) [4] can not be employed into MCS due to the heavy communication over- head.1 Secondly, although modern mobile devices, such as mobile phones and tablets, have significantly improvement in terms of 2 computing capability, they still cannot compete with personal computers or other powerful devices. Com- plicated computation also reduces the battery life of mobile devices. Therefore, some schemes based on fully homomor- phic encryption (FHE) [19] or multi-layer onion additively homomorphic encryption [20] are also not suitable for M- CS due to complex clientside encryption and decryption computation, although they circumvent the communication lower bound and achieve constant communication band-

width overhead. Thirdly, many existing oblivious schemesare also suffered by the lager minimum effective item size. Minimum effective item size refers to the minimal number of bits in an effective item of an oblivious scheme required to meet the predefined communication complexity (constant or logarithmic). Lager item size prevents the mobile client from fine-grained accessing its own data. Moreover, it also further increases the communication or computation overhead of existing oblivious schemes.

II. RELATED WORKS

All the correlated works that have been done that are related to the current problem are follows. [1] M. S. Islam, M. Kuzu, and M. Kantarcioglu, "Access pattern disclosure on searchable encryption: Ramification, attack and mitigation," in 19th Annual Network and Distributed System Security Symposium, NDSS 2012, San Diego, California, USA, February 5-8, 2012, 2012. [Online]. Available: https://www.ndss-symposium.org/ndss2012/ 18-20, 2009. Proceedings, 2009, pp. 196–214. [Online]. Available: https://doi.org/10.1007/978-3-642-00468-1 12O. [4]Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious rams," J. ACM, vol. 43, no. 3, pp. 431–473, 1996. [Online]. Available: http://doi.acm.org/10.1145/ 233551.233553..[6] T. Hoang, A. A. Yavuz, F. B. Durak, and J. Guajardo, "Oblivious dynamic searchable encryption via distributed PIR and ORAM," IACR Cryptology ePrint Archive, vol. 2017, p. 1158, 2017. [Online]. Available: http://eprint.iacr.org/2017/1158. [7] S. Garg, P. Mohassel, and C. Papamanthou, "TWORAM: efficient oblivious RAM in two rounds with applications to searchable encryption," in Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part III, 2016, pp. 563–592. [Online]. Available: https://doi.org/10.1007/978-3-662- 53015-3 20.

III. PROBLEM DEFINITON

In existing system, the cloud is not considered fully trusted. Thus, the client may employ encryption schemes to keep data confidential before uploading it to the cloud. The data outsourced to a cloud must be secured. Unauthorized data access by other users and processes (whether accidental or deliberate) must be prevented as discussed above, any weak entity can put the whole cloud at risk. In such a scenario, the security mechanism must substantially increase. However, in MSC-based applications, data always be related to certain information, such as location information in location based services. In this situation, which item of data is being accessed leaks addition information to the cloud server.

The data compromise may occur due to attacks by other users and nodes within the cloud. • The employed security strategy must also take into account the optimization of the data retrieval time. • Data loss • Time delay from server

IV. PROPOSED SYSTEM

In this paper, we collectively approach the issue of security and performance as a secure data replication problem. We present Detaching and Reproducting of Data in the Cloud for Excellent Performance and Security that judicially fragments user files into pieces and replicates them at strategic locations within the cloud. The division of a file into fragments is performed based on a given user criteria such that the individual fragments do not contain any meaningful information. Each of the cloud nodes contains a distinct fragment to increase the data security. In addition store in different server so in future some Server is not available are Hacked we can get back our original data from remaining Server. The second is to forward the data to others in secure manner. So the user request to forward the data from cloud to others mean the server generates a key for a specific file and provided to the cloud user. The random function used to generate a key. The keys are shared by the sender and receiver. By using the secret key the receiver can fetch data from the cloud securely.

Cost Efficient & data Protection in cloud is good. • To improve data retrieval time, the nodes are selected based on the centrality measures that ensure an improved access time. Proposed an efficient, secure and privacy-preserving mobile cloud storage scheme

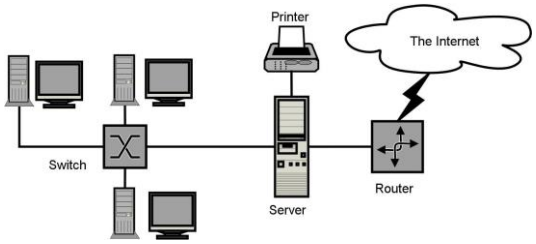


Fig 1. Cloud Computing

A. User Authentication

User Authentication is the process of identity verification you are trying to prove a user is who they say they are. For a user to prove their identity, a user needs to provide some sort of proof of identity that your system understands and trust. The authentication process starts with creating an instance of the Login Context

B. Fragmentation

In our second Module, We are splitting the file in to small fragments. Once the file is split into fragments, this concept selects the cloud nodes for fragment placement. The selection is made by keeping an equal focus on both security and performance in terms of the access time. The process is repeated until all of the fragments are placed at the nodes. Partial Replication represents the fragment placement methodology. Mainly we focus on the storage system security in this work. As stated above, the probability of a successful coordinated attack is extremely minute

C. Data upload& Data Encryption

This component supports the upload by invoking and managing their execution based on the client's requirements. Client uploaded data are encrypted for secure data storage in cloud. Encrypted data are stored in different virtual server with fragments. In this

module, we are fragments by the Fs algorithm. By using this algorithm, Once the user requested for the information, It will retrieve the necessary fragments in the sequential order. Once all the fragments are collected, will produce an entire information to the user.

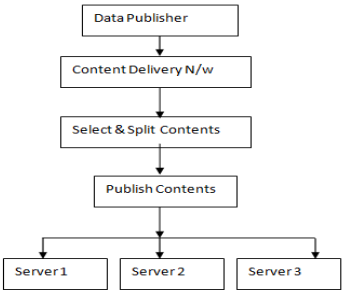
D. Server Analysis

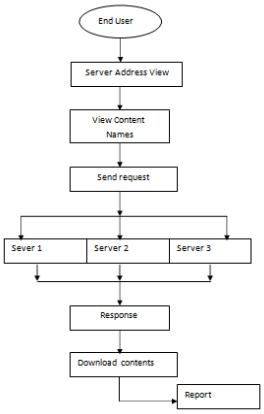
The task of offering fault analysis as a service requires the service provider to realize generic fault analysis mechanisms such that the client's applications deployed in virtual machine instances can transparently obtain server status properties. To this aim, we define *ft−unit* as the fundamental module that applies a coherent server analysis mechanism to a recurrent system failure at the granularity of a VM instance.

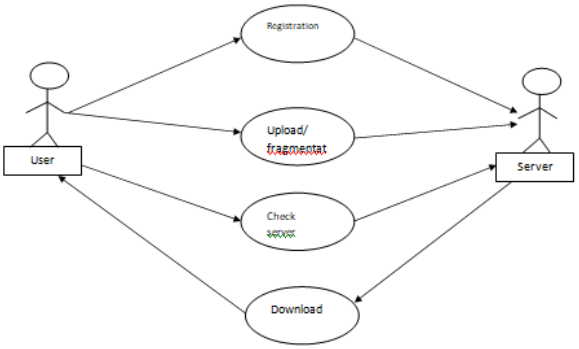
E. Data Retrieval and Decryption

The data retrieval module describe the retrieve data from different virtual server only authenticate user. Data are encrypted in different virtual server with fragments. Data are retrieved from different virtual server and combine the data and convert to decrypted format. Decrypted data are bringing to original data for user extraction. The goal of this component is to achieve system- level resilience by minimizing the downtime of the system during failures. To this aim, this component supports ft−units that realize recovery mechanisms so that an error-prone node can be resumed back to a normal operational mode.

V. ARCHITECTURAL DIAGRAMS







VI. SOFTWARE SPECIFICATIONS

A. The .NET Framework

Microsoft designed C# from the ground up to take advantage of its new .NET Framework. Because C# is a player in this new .NET world, you should have a good understanding of what the .NET Framework provides and how it increases your productivity. The .NET Framework is made up of four parts, as shown in the Common Language Runtime, a set of class libraries, a set of programming languages, and the ASP.NET environment. The .NET Framework was designed with three goals in mind. First, it was intended to make Windows applications much more reliable, while also providing an application with a greater degree of security. Second, it was intended to simplify the development of Web applications and services that not only work in the traditional sense, but on mobile devices as well. Lastly, the framework was designed to provide a single set of libraries that would work with multiple languages. The following sections examine each of the .NET Framework components.

WEB DEVELOPMENT:

The .NET Framework was designed with one thing in mind: to fuel Internet development. This new fuel to add to Internet development is called *Web Services*. You can think of Web Services as a Web site that interacts with programs, rather than people. Instead of delivering Web pages, a Web Service takes a request formatted as XML, performs a particular function, and then returns a response to the requester as an XML message. Note XML or eXtensible Markup Language is a self describing language much like that of HTML. XML on the other hand has no predefined tags thus allowing it great flexibility in representing a wide variety of objects.

A typical application for a Web Service would be to sit as a layer on top of a corporate billing system. When a user surfing the Web purchases products from your Internet site, the purchase information is then sent to the Web Services, which totals all the products, adds a record to the accounts receivable database, and then returns a response with an order confirmation number. Not only can this Web Service interact with Web pages, it can interact with other Web Services, such as a corporate accounts payable system.

In order for the Web Service model to survive the natural evolution of programming languages, it must include much more than a simple interface to the Web. The Web service model also includes protocols that enable applications to find Web Services available across a LAN or the Internet. This protocol also enables the application to explore the Web Service and determine how to communicate with it, as well as how to exchange information. To enable Web Service discovery, the Universal Discovery, Description and Integration (UDDI) was established. This allows Web Services to be registered and searched, based on key information such as company name, type of service, and geographic location.

Application Development

Aside from Web development, you can still build traditional Windows applications with the .NET Framework. Windows applications created with the .NET Framework are based upon *Windows Forms*. These Windows Forms are somewhat of a crossbreed between Visual Basic 6 forms and the forms of Visual C++. Though forms look the same as their predecessors, they are completely object-oriented and class-based, much like form objects in the Microsoft Foundation Class. These new Windows Forms now support many classic controls found in Visual Studio, such as the Button, TextBox, and Label, as well as ActiveX controls. Aside from the traditional controls, new components such as PrintPreview, LinkLabel, ColorDialog, and OpenFileDialog are also supported. Building applications with .NET also provides you with many enhancements not found in other languages, such as security. These security measures can determine whether an application can write or read a disk file. They also enable you to embed digital signatures into

The application to ensure that the application was written by a trusted source. The .NET Framework also enables you to embed component information, and version information, within the actual code. This makes it possible for software to install on demand, automatically, or with no user intervention at all. Together, all of these features greatly reduce support costs within the enterprise.

Common Language Runtime

Programming languages usually consist of both a compiler and a runtime environment. The compiler turns the code that you write into executable code that can be run by users. The runtime environment provides a set of operating system services to your executable code. These services are built into a runtime layer so that your code does not need to worry about the low-level details of working with the operating system. Operations such as memory management and file I/O are good examples of services that might be provided by a runtime environment. Before .NET came along, each language shipped with its own runtime environment. Visual Basic shipped with a runtime called MSVBVM60.DLL. Visual C++ shipped with a DLL called MSVCRT.DLL. Each of these runtime modules provided a set of low-level services to code that developers wrote. Developers would write code and then build that code with the appropriate runtime in mind. The executable code would ship with the runtime, which would be installed on a user's machine if it weren't already present.

.NET CLASS LIBRARIES

Developers like to work with code that has already been tested and shown to work, such as the Win32 API and the MFC Class libraries. Code re-use has long been the goal of the software development community. However, the practicality of code re-use has not lived up to expectations. Many languages have had access to bodies of pre-tested, ready-to-run code. Visual C++ has benefited from class libraries such as the Microsoft Foundation Classes (MFC), which enabled C++ developers to build Windows applications quickly, and the Active Template Library (ATL), which provided support for building COM objects. However, the languagespecific nature of these libraries has made them unavailable for use in other languages.

Visual Basic developers are locked out of using ATL when building their COM objects. The .NET Framework provides many classes that help developers re-use code. The .NET class libraries contain code for programming topics such as threading, file I/O, database support, XML parsing, and data structures, such as stacks and queues. Best of all, this entire class library is available to any programming language that supports the .NET Framework. Thanks to the CLR, any .NET language can use any class in the .NET class library. Because all languages now support the same runtime, they can re-use any class that works with the .NET Framework. This means that any functionality available to one language will also be available to any other .NET language.

The class library re-use picture painted by the .NET Framework gets even better when you realize that re-use extends to your code, not just code that Microsoft ships with .NET. The code that Microsoft ships in the .NET class library code base is architecturally no different from the code you write. The Microsoft code is simply code that was written using a language supported by

.NET and built using a .NET development tool. This means that Microsoft is using the same tools that you will use to write your code. You can write code that can be used in other .NET languages, just as Microsoft has with its class library. The .NET Framework enables you to write code in C#, for example, and hand it off to Visual Basic .NET developers, who can use your compiled code intheir applications.

B. Sql server

SQL Server 2005 is the successor to SQL Server 2000. It included native support for managing XML data, in addition to relational data. For this purpose, it defined an xml data type that could be used either as a data type in database columns or as literals in queries. XML columns can be associated with XSD schemas. XML data being stored is verified against the schema. XML is converted to an internal binary data type before being stored in the database. Specialized indexing methods were made available for XML data. XML data is queried using XQuery. Common Language Runtime (CLR) integration was a main feature with this edition, enabling one to write SQL code as Managed Code by the CLR. SQL Server 2005 added some extensions to the T-SQL language to allow embedding XQuery queries in T-SQL. In addition, it also defines a new extension to XQuery, called XML DML that allows query-based modifications to XML data.

Managing Services

- SQL Server
- SQL Server Agent
- SQL Server Browser
- SQL Server Integration Services
- SQL Server Anaylysis Services

SQL Server Management Studio

This tool is a new feature in SQL Server 2005. It replaces Enterprise Manager and Query Analyzer from earlier versions. It has been developed using a Visual Studio shell as a base. It follows the paradigm of Visual Studio, in which most tools are organized as tabbed, dockable, orfloating windows.

The registered server's pane allows viewing and managing parameters for connecting to servers. The tool includes both script editors and graphical tools which work with objects and features of the server.A central feature of SQL Server Management Studio is the Object Explorer, which allows the user to browse, select, and act upon any of the objects within the server.

SQL Server 2005 Features

- Database mirroring
- *T-SQL (Transaction SQL) enhancements*
- CLR integration
- Service Broker

Ease of Installation, Deployment, and Use

SQL Server includes a set of administrative and development tools that improve ability to install, deploy, manage, and use SQL Server across several sites.

Scalability

The same database engine can be used across platforms ranging from laptop computers running Microsoft Windows® 95/98 to large, multiprocessor servers running Microsoft Windows NT®, Enterprise Edition.

Data Warehousing

SQL Server includes tools for extracting and analyzing summary data for online analytical processing (OLAP). SQL Server also includes tools for visually designing databases and analyzing data using English-based questions. In this project SQL server is used because of the above features.

VII. TESTING

A. Feasibility study

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential. The feasibility study investigates the problem and the information needs of the stakeholders. It seeks to determine the resources required to provide an information systems solution, the cost and benefits of such a solution, and the feasibility of such a solution. The analyst conducting the study gathers information using a variety of methods, the most popular of which are: Interviewing users, employees, managers, and customers. Developing and administering questionnaires to interested stakeholders, such as potential users of the information system. Observing or monitoring users of the current system to determine their needs as well as their satisfaction and dissatisfaction with the current system. Collecting, examining, and analyzing documents, reports, layouts, procedures, manuals, and any other documentation relating to the operations of the current system. Modeling, observing, and simulating the work activities of the current system. The goal of the feasibility study is to consider alternative information systems solutions, evaluate their feasibility, and propose the alternative most suitable to the organization

B. Economic feasibility

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely

available. Only the customized products had to be purchased.

C. *Technical feasibility*

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

D. *Social feasibility*

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

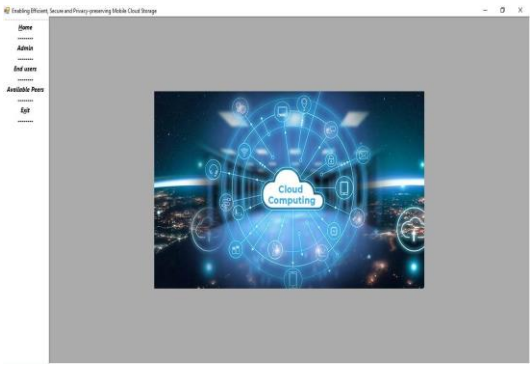
E. *Operational feasibility*

The ability, desire, and willingness of the stakeholders to use, support, and operate the proposed computer information system. The stakeholders include management, employees, customers, and suppliers. The stakeholders are interested in systems that are easy to operate, make few, if any, errors, produce the desired information, and fall within the objectives of the organization.

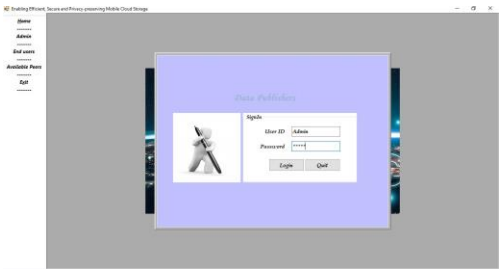
VIII. CONCLUSION

In this paper, we propose an efficient, secure and privacy- preserving mobile cloud storage (MCS). The proposed scheme can protect data and access pattern simultaneously. Compared with existing schemes. We also take temporal locality into consideration to further improve the efficiency of the scheme. The security and privacy proofs and analyses show that our scheme achieves data confidentiality and sufficient privacy preservation level. Finally, we compare our scheme with other two oblivious storage schemes and fully estimate our construction in a simulation environment. The results indicate that our scheme is significantly efficient and has goodperformances.

IX. OUTPUT SCREENS

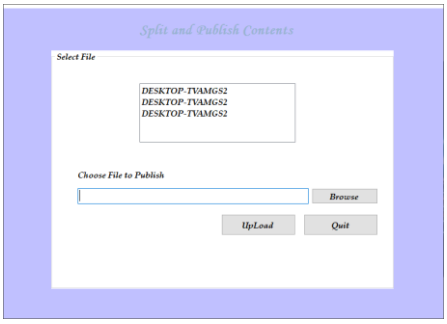


Home Screen

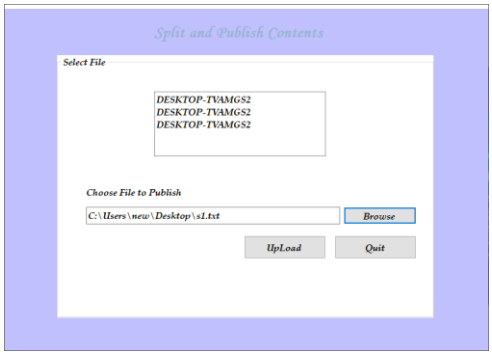


Sign in Page

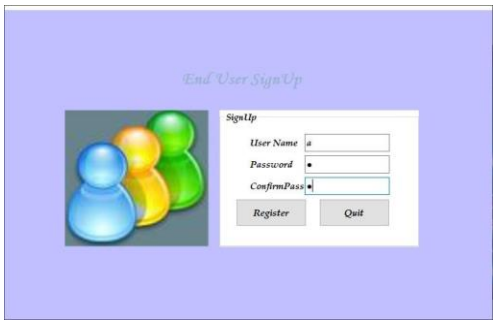
Cloud Servers Page



Split & Publish Contents Page



Select The File



Log In Page

Available Data to Download Page

REFERENCES

[1] M.S. Islam," Access pattern disclosure on searchable encryption: Ramification attack mitigation", Symposium, NDSS 2012, california, 18029,2009.

[2] J.Killian,"Founbding cryptography on oblivious transfer", ACM Symposium on Theory of Compuiting, May 2-4, 1988, Chicago, Illinois, pp 20-26.

[3] D. Boneh, D. Mazirees, and R.A.Popa, " Remote oblivious storage : Making oblivious ram practical." Pp1-18,2011

[4] O.Goldreich and R. Ostrovesky, " Software protection and simulation on oblivious rams", ACM, volo. 43 23351.52

[5] J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy, "Blind and anonymous identity-based encryption and authorised private searches on public key encrypted data," in Public Key Cryptography - PKC 2009, 12th International Conference on Practice and Theory in Public Key Cryptography, Irvine, CA, USA, March18-20, 2009. Proceedings, 2009, pp. 196–214. [Online]. Available:https://doi.org/10.1007/978-3-642-00468-1 12

[6] Ainul Husna Mohammed Yusuf, " Classification of Fall Detection System for Elderly : Systematic Review", TURCOMAT, vol. 12, no 3, 2021.

[7] I. Kim, K. Kim,T. Seo and M. Ko, "A study on an ICT based system for safe management of agricultural facilities for farmers' safety activities", J. Ergonom Soc. Korea,vol 37,no 4,pp 489-502,2018.