**INTRODUCTION**

According to the Forrester research says” The global cloud computing market is anticipated to rise from $272billion in 2018 to $624billion by 2023 at a compound annual growth rate of 18%, a report from research and markets showed[1]. Cloud computing is an advanced technology every person is used inner or outer in today’s world [2]. The advance and rapidly expanding technology of cloud computing are used computation and storage. The very minimum cost is used storage and computation as a service in it. Service model provided three essential services in it: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service(SaaS)[3]. The NIST definition, “Cloud computing is a model permissive ubiquitous, convenient, on-demand network approach to a shared pool of configurable computing property(e.g. networks, servers, storage, applications, and services) that can be immediately provisioned and released with basic management effort or service provider interaction [4][6]. Cloud storage is a crucial service of cloud computing[5]. They involve data privacy, data protection, data availability, data location, and, secure transmission which is a crucial release in cloud security. The involved in cloud challenge security are threats, data loss, degradation, outside malicious attack and multi-tenancy [6].

The stored information of integrity is conserved for data integrity in the cloud system. The unauthorized users should not be accessed misappropriate or vary of data. Data integrity and reliability of data are faithful to preserve by the cloud computing provider. Data confidentiality is also a crucial way from a user’s point of perspective therefore they store their private or confidential data in the cloud. Data confidentiality is taken to assure access control policies and authentication. The faith of cloud computing could be forward by rising cloud authenticate and data confidentiality. So the keep data on the cloud should be security, integrity, privacy, and confidentiality of crucial demands from the user perspective[7].

A secure data storage of cloud computing is presented of a data auditing scheme. Auditing is a refinement of checking the user data which can be done by the data owner or by a TPA[8]. The integrity of stored data on the cloud serves to maintain it. The TPA manage is split into two: one is private audibility, which allows the data owner can analyze the integrity of the data. No one has the authority to inquire about the server considering the data[8]. Though it attains to increases verification overhead of the user. Second is public audibility, the confidentiality of the data can check by only TPA. The behalf of the client can act TPA so TPA is an entity. The verification of integrity has handled to appropriate work that all essential expertise, capabilities, knowledge and professional skill and the position of the client is also reduced by it[8]. It should be crucial that TPA should efficiently or frequently audit the cloud data storage without requesting for the local copy of data[9]

The security issues sparked the mechanism to control access to the network in order to protect it from intruders [1]. A vulnerability in a web application can be opening way for an attack in the whole information system and does not close the possibility for the control server [2]. One feature of the login feature is to authenticate users as identity checks where this function becomes an essential component of the security system. This is a way to differentiate between registered users and intruders. Authentication users on a network is a must for many companies that seriously protect their information assets and to know who and what will be accessed on their networks. Various kinds of techniques for increase security data or information already is developed, one common way is by cryptographic or encryption techniques [3]. Use of encryption is needed to support the security of the login process. The sample web-based application used has been

applied encryption method using Message Digest 5 (MD5) method so it must be updated using another more reliable method. The SHA algorithm has a difference in the size of each block, the word of the data used during the hashing process, the length of the message can be processed, and the size of the resulting message digest varies according to the algorithm used. SHA 1 has a 264-1 message input capacity, with 160 bits of hash results and 280 hash power evaluations. Finally, in 2005 Rijmen and Oswald published an attack on the reduced SHA 1 version (using only 53 rounds from 80 rounds) and the results were found the collision with a complexity of about 280 operations [4]. SHA 256 and 384 are not used much even

though for security due to a protracted process that causes the length of time in hashing [4]. SHA 512 is a development of SHA 1 which is an MD4 based improvement. According to Megah Mulya [5], 2009, the reliability of SHA 512 is

achieved by the ability to generate 512-bit hash values, which is the longest hash value that a hash function can generate. This long hash value makes the SHA 512 more resistant to attack than any other hash function so SHA 512 is considered a powerful, robust and fast hash function. The SHA 512 algorithm is an algorithm that uses the one-way hash function created by Ron Rivest. This algorithm is the development of previous algorithms SHA 0, SHA 1, SHA 256 and SHA 384 algorithms. Journal of research Christian Angga [9], 2007, explains how the cryptographic algorithm of SHA 512 is receiving input in the form of messages of any size and generates message diggest which has 512-bit length.

Its predecessor is SHA1, and MD5 which is a renewal of MD4, the linkage, and development of the hash algorithm, indicating that the algorithm has proven to have been found to be a collision vulnerability. Currently, the National Institute of Standards and Technology (NIST) has made SHA 224, SHA 256, SHA 384, and SHA 512 as the new standard hash function.

This section will explain the systematic way used to solve the research problem and also the steps undertaken in the testing and analysis of this research. The stages consist of literary studies is to analyze the system used to determine the current conditions, needs, advantages, and disadvantages of these programs. This stage is done by reading several books, previous research journals, papers or articles that are appropriate or relevant as well as collecting resources from the internet both journals, websites, proceedings and source code that can be used in this research.

Needs analysis and system vulnerabilities are carried out to analyze the vulnerabilities and needs of the system used. The analysis is focused on the web-based application login system encryption function which aims to find out the advantages and disadvantages of the encryption method currently used when replaced using the latest algorithm method. Needs analysis and design for improvement are to describe and display an overview of the encryption process when the login is done. The description carried out is by showing a flowchart and conceptual diagram so that the work process in which password encryption is carried out until the login activity occurs can be delivered and understood more clearly.

Mitigation performed with the implementation of the latest hash function algorithm calling the method, code change for patching and test results from implementation. Testing in this study was conducted to show a comparison between the use of MD5 encryption method and SHA 512 encryption method. Testing was done by Penetration Testing and User Acceptance Test. Penetration Testing is done by Brute Force testing while User Acceptance Test is done by filling out a questionnaire that is used as one of the recommendations to improve data security in web-based applications.