iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4660

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

Symmetric Groups of Authentications and Key Management with Session Based Automated Key Updation

K. Gunalan[1], P. Mallika[2], A. Gokilavani[3]
[1] *ME 4th Semester, Department of CSE, Jai Shriram Engineering College/Tirupur/TN*
[2,3] Assistant *Professor, Department of CSE, Jai Shriram Engineering College/Tirupur/TN*

Abstract : Authenticated key exchange (AKE) is one of the most important applications in applied cryptography, where a user interacts with a server to set up a session key where pre-registered information (aka. authentication factor), such as a password or biometrics, of the user is stored. While single-factor AKE is widely used in practice, higher security concerns call for multi-factor AKE schemes, e.g. combining both passwords and biometrics and device simultaneously. However, in some schemes, security is even weakened in the sense that leakage of one authentication factor will defeat the whole authentication process. Furthermore, an inevitable by-product arises that the usability of the protocol often drops greatly. To summarize, the existing multi-factor protocols did not provide enough security and efficiency simultaneously. Here, we make one step ahead by proposing a very efficient authentication method. We define the security model and give the according security analysis. To overcome the security issues proposed method implements textual, graphical, and biometric and device password to access the user accounts and an efficient AES algorithm for data transaction which is more secured algorithm is used.
Keywords-AKE, Encryption Algorithms, Secure MFAKE, AES, RSA, Triple Des, Multi-Factor Key Encryption, VPN, E2FA, TOTP, Unclonable.

I. INTRODUCTION

At the time of systems are connected through the network, attacks are possible during transmission time Network security is a process that is designed to detect, prevent and recover from a security attacks User authentication is a very important part for many information systems. The authentication service is concerned with assuring that a communication is authentic. It helps to prove that the source entity only has involved the transaction. Key exchange protocols allow two or more parties communication over a public network to establish a common secret key called a session key. Due to their significance in building a secure communication channel, a number of key exchange protocols have suggested over the years for a variety settings. In order to avoid mistakes and impersonations during the process we can use various authentication means. It is often done via the following methods -Textual Authentication is the most popular way, while quite insecure in some cases. The statistics show that most passwords in use are not so hard to guess. Secret Hardware Key Based Authentication provides higher security than password with storage space for long secret keys and computation power for authentication. But if it is stolen or lost, the authentication fails completely.Genetic Authentication utilizes the unique and life-long invariant property of the biometrics. But it is not so reliable.Combining all these processes together is called the Multi Factor Authentication Key exchange (MFAKE) protocol.

II. FUNCTIONS OF MFAKE PROTOCAL

For a secured data transaction, before transferring the data few authentication steps are followed. The user needs to complete all the authentication steps to send/receive a data. The authentications steps generally involve three steps. They are the above discussed process, password based textual authentication, a hardware device with a serial key and the unclonable biometric password. These steps are used in order to authenticate the user and for a secured data transaction Phishing can be combated by protocols that provide strong, easy-to-use server-to-client authentication. Password-authenticated can make server-to-client authentication easier and resistant to offline dictionary attacks, and additionally provides a secure key for encryption. Graphical password is more difficult to defend against. If a user's computer is compromised by passive spyware that records keystrokes and occasionally transmits this information to an attacker's server, then the use of one-time passwords may be effective, since a previously used one-time password cannot be used again. In Biometric passwords are users can never lose their biometrics, and the biometric signal is difficult to steal or forge. With storage space for long secret keys and computation power for authentication, hardware provides higher

©IJRASET: All Rights are Reserved

security than password. To reduce the damage caused by compromising an authentication factor, many organizations with high security requirements – such as financial institutions, governments, and corporate virtual private networks (VPNs) – are deploying multi-factor authentication, which depends on a variety of attributes, or factors. The factors could include: a long-term password, a set of one-time passwords, a private key, or a biometric. For example, one-time passwords cannot all be compromised unless one obtains the sheet of paper listing all the one-time passwords or the device generating the one-time passwords, whereas a biometric read by a trusted device (such as a secure fingerprint reader) should not be able to be reproduced without the presence of the person in question (or at least their figer).

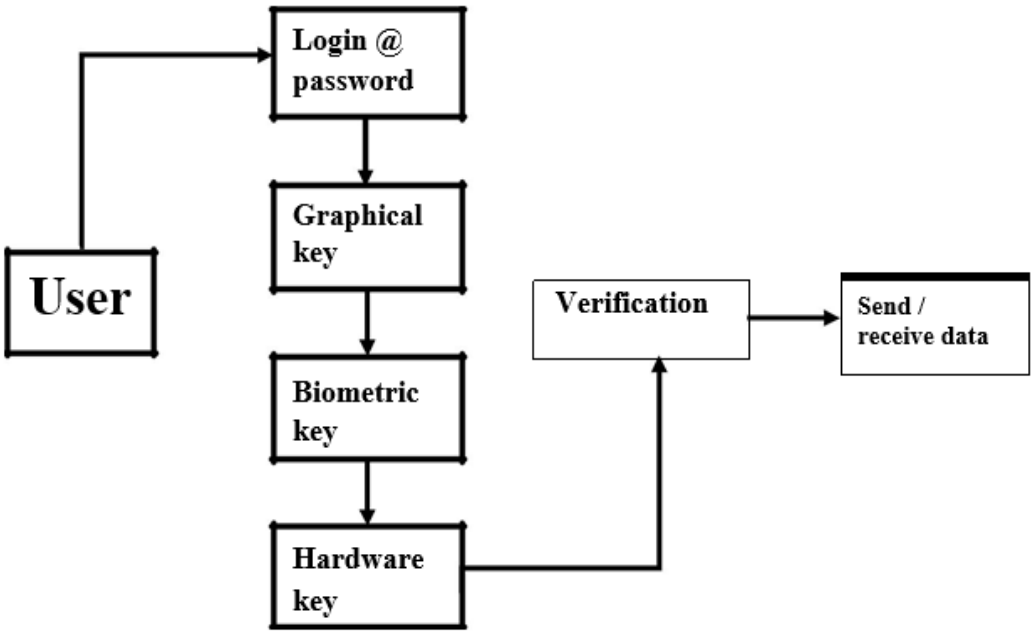


Fig. 1. Block Diagram of The Over all System.

III. NEED FOR MFAKE PROTOCAL

Single-factor authentication only provides limited security, then combining these methods together is considered as a good way to achieve higher security.This again, raised the need for secure multi-factor authentication schemes. In general, there are several issues like efficiency, Robustness, privacy, session key agreement and usability which should be addressed by multi-factor authentication schemes. Multi-factor authentication can provide an enhanced level of assurance in higher-security scenarios such as online banking, virtual private network access, and physical access because a multi-factor protocol is designed to remain secure even if all but one of the factors has been compromised.

A. The multifactor authentication supports the following constraints

1) *Robustness:* Whenever there is one factor uncorrupted, the authentication scheme should remain secure.
2) Which is a basic security requirement for multi-factor authentication. But many existing schemes could not meet it sing redundant authentication, even worse, introducing more weakness.
3) *Privacy:* Biometric characteristics are acknowledged as one kind of privacy information, so which must be protected to avoid leakage. In addition, the leakage of biometric will not only break the security in the authentication, but also a lead to further social damage.
4) *Session Key Agreement:* Authentication is just a way to prevent illegal users from entering a system. While the subsequent communications also need to be protected. So it is ideal to set up a session key between the client and server by the end of an authentication.
5) *Usability:* The participation of people requires the authentication schemes be friendly to use: e.g., most people annot remember long and random passwords, and hate to carry many different devices, even taking long and random enough passwords and more different devices can improve the security.

Mutifactor authentication smoothly supports the emerging network security properties that are embedded with sensors to enable them to send/receive data.

©IJRASET: All Rights are Reserved

IV. EXISTING WORK

A. Login Security

1) Two factor authentication is commonly used for login security; combining any two authentication methods.

2) The login data are stored in the database instantly.

B. Transaction Platform

1) Data is transferred even when the receiver is offline

2) The data is transferred in an encrypted format using 3DES algorithm.

V. PROPOSED SYSTEM

A. Secured Messages Communication Framework

The common and simple perception of network security at the beginning had two constraints. First is the signup security with a very strong key which makes hacking more difficult. Second is the data transaction with a highly efficient encryption and decryption techniques. Combination of these two makes a secured message communication.

1) *Higher Security:* Provides higher secured communication and avoids different kinds of attacks to the maximum.

2) *Session Key Implementation:* Data can be transferred from the sender to the receiver using session keys.

3) *Login Security:* Multifactor Authentication like textual, graphical, and biometric and USB device passwords are being implemented which provides login security.

4) *Resistant to Attacks:* AES is strongly resistant to differential, truncated differential, linear, interpolation and Square attacks.

5) *Strong Keys Generated:* The keys generated are very strong that the time required to check all possible keys at 50 billion keys per second in AES for a 128-bit key is 5 x 1021 years.

VI. SYSTEM DESIGN

Design is multi-step process that focuses on data structure software architecture, procedural details, (algorithms etc.) and interface between modules. The design process also translates the requirements into the presentation of software that can be accessed for quality before coding begins. Computer software design changes continuously as new methods; better analysis and broader understanding evolved. Software design is at relatively early stage in its revolution. Therefore, software design methodology lacks the depth, flexibility and quantitative nature that are normally associated with more classical engineering disciplines. However techniques for software designs do exist, criteria for design quality are available and design notation can be applied.

A. Input Design

Input Design is the process of converting a user-oriented description of the inputs to a computer based business system into a program-oriented specification.

The objectives in the input design are,

To produce a cost efficient method of input.

To achieve a highest possible level of accuracy.

To ensure that input is acceptable and to be understood by the user.

Several activities have to be carried out as a part of the overall input process. They include

1) *Data Recording:* Collection of data at its source.

2) *Data Description:* Transfer of data to an input form.

3) *Data Conversion:* Conversion of the data to a computer acceptable medium.

4) *Data Verification:* Checking the conversion

5) *Data Control:* Checking the accuracy and controlling the flow of data to the computer.

6) *Data Transmission:* Transmission or transferring the data to the computer.

7) *Data Validation:* Checking the input data by program when it enters the computer system.

8) *Data Correction:* Correcting the error that is found at any early stages.

B. Output Design

Output design generally refers to the result and information that are generated by the system for many end-users; output is the main reason for developing the system and the basis on which they evaluate the usefulness of the application. In any system, the output design determines the input to be given to the application. The output design is an ongoing activity almost from the beginning of the project, and follows the principles of form design. Effects and well define an output

©IJRASET: All Rights are Reserved

design improves the relationships of system and the user, thus facilitating decision-making. A major form of output is a hard copy from the printer, however soft copies are available.

The types of output used in the system are,

1) *Internal Output:* where destination is within the organization and is the user's main interface with the computer.
2) *Interactive Output:* This involves the user in communication directly with the computer.
3) *External Output:* whose destination is output, the organization and which require special attention since they project the image of the organization.

VII. SYSTEM ARCHITECTURE

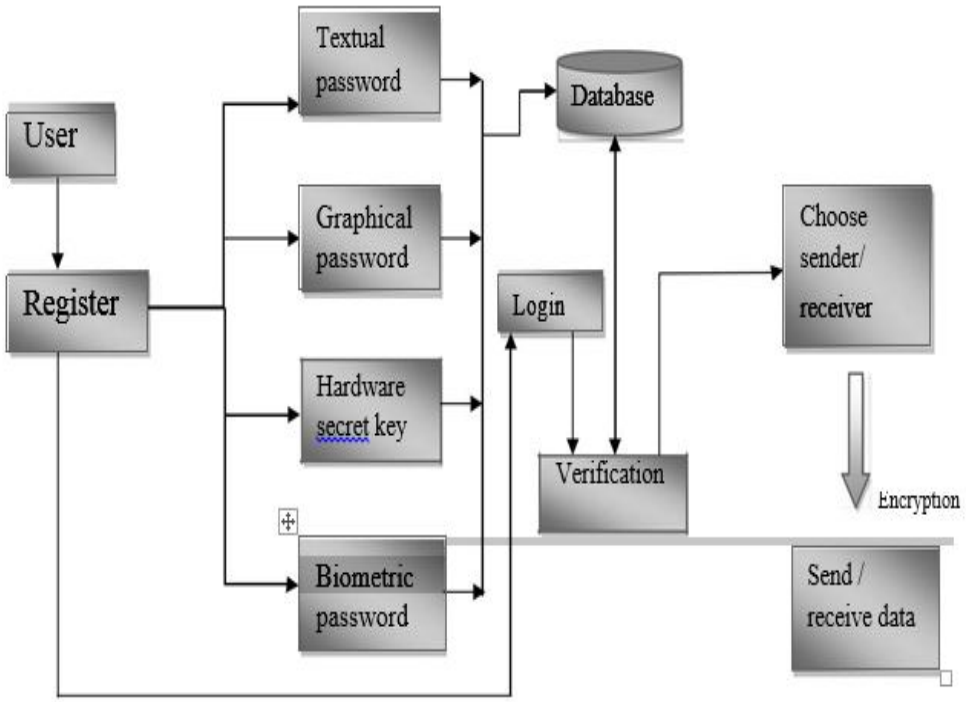


Fig. 2. **Arhitecture Diagram.**

A. *Architecture Description*

A system architecture or system architecture is the conceptual design that defines the structure and/or behavior of a system. An architecture description is a formal description of a system, organization in a way that supports reasoning about the structural properties of the system. It defines the system components or building blocks and provides a plan from which products can be procured, and system developed, that will work together to overall system. This may enable one to manage investment in a way that meets business needs. The fundamental organization of a system, embodied in its components, their relationship to each other and the principles governing its design and evolution. The composite of the design architectures for products and their life cycle process. A representation of the system in which there is a mapping of functional onto hardware and software components, a mapping of the software architecture onto hardware architecture, and human interaction with these components. An allocated arrangement of physical elements which provide the design solution for a consumer product or lifecycle process intended to satisfy the requirement of the functional architecture and the requirements baseline. Architecture is the most important, pervasive, top-level, strategic invention, decision and their associated rationales about the overall structure and associated characteristics and behavior.

B. *Modules:* Modules are units of code written in access basic language. We can write and use module to automate and customize the database in very sophisticated ways. The respective modules for a secured message communication are:

©IJRASET: All Rights are Reserved

User registration
Authentication
Data transmission

1) *User Registration*: The User Registration has both the sender and receiver registration process. Initially they have to register for their interaction between them. The sender and receiver registered by using the individual textual passwords. The Registration process is common for both the sender and receiver. During the registration phase the user have to register the hardware security key and their finger print. These registered values are stored in database for security verification purposes while the login process**.**

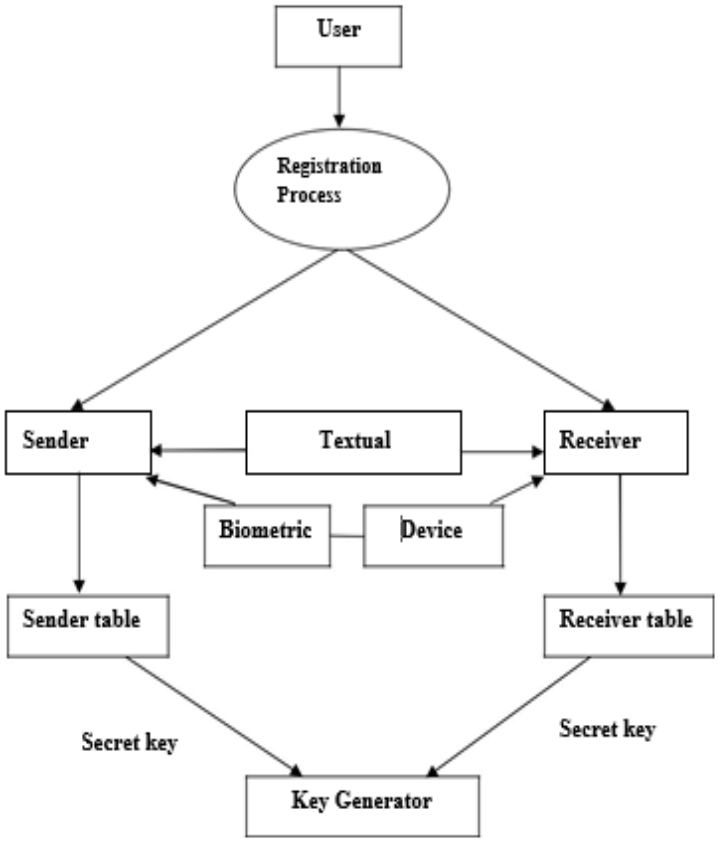


Fig.3. Registration Block Diagram for Sender and Receiver.

The registered data of both sender and receiver is stored in the data base automatically. After registration both the sender and receiver logs in together and the data is transferred.

2) *Authentication:* The authentication process undergoes four steps. Authentication is done after user registration. The four steps are,

Textual authentication
Graphical authentication
Hardware authentication
Biometric authentication

a) *Textual Authentication:* The user first registers with a simple textual security password and with a serial key. After registration the first steps is to verify whether the user is an authentic user or not, by checking the user name, the textual password and the serial key. This is the first step of authentication.

b) *Graphical Authentication:* This step is used to login the individual sender and receiver. This graphical password is created by using the information about the sender and receiver and with the help of sessions using in it and is sent to the user registered phone number. These passwords are accessed only in the particular location of the secured image. The graphical

©IJRASET: All Rights are Reserved

password is generated based on the users clicking point which is based on the corresponding x axis and y axis value. If the values of the clicking point match with the registered value, only the user can login and process this system. After finding the coordinates a text box will be displayed and the graphical password should be entered.

c) *Biometric Password Authentication:* This step is used to generate the biometrics scheme for the authenticated data. Registered finger print value is checked with the current fingerprint of the person who tries to login. This is done by checking pixel by pixel of the registered fingerprint and current user fingerprint. By using this biometrics the data is being prevented. The sender and receiver perform the data transaction by using biometrics scheme. So the system is full secured.

d) *Hardware-Based Authentication:* With storage space for long secret keys and computation power for authentication, hardware provides higher security than password. Here it is authenticated using USB device.

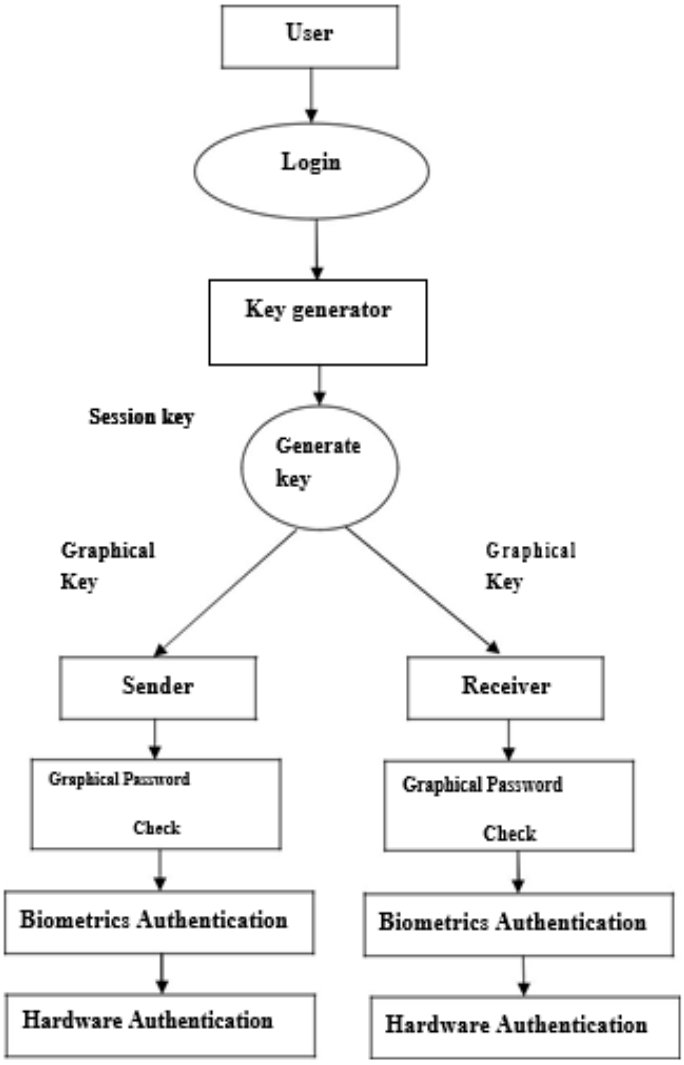


Fig. 4.Authentication Block Diagram for Sender and Receiver.

3) *Data Transmission:*

The two phases in the data transmission are,

Data transmitting

Data receiving

a) *Data Transmitting:* After the multifactor authentication the sender begins to send the data. The sender sends the data to the receiver in the encryption format for the security purpose. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. The encryption process is done by AES algorithm. The data's are encrypted so the unknown person can't access the files which are sent by

©IJRASET: All Rights are Reserved

sender. These encryptions are known only by the authorized sender. AES is considered one of the most efficient algorithms currently available.

b) Data Receiving: After the sender sends the data the receiver access the data using the session password. Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. After finishing multifactor authentication the receiver can decrypt and view the original format of the data which has sent by the sender. Authorized person can only decrypt the file using the key. So the file is prevented from unauthorized access. The data transmission is the last step of the secured message communication framework using the multilayered authentication mechanism

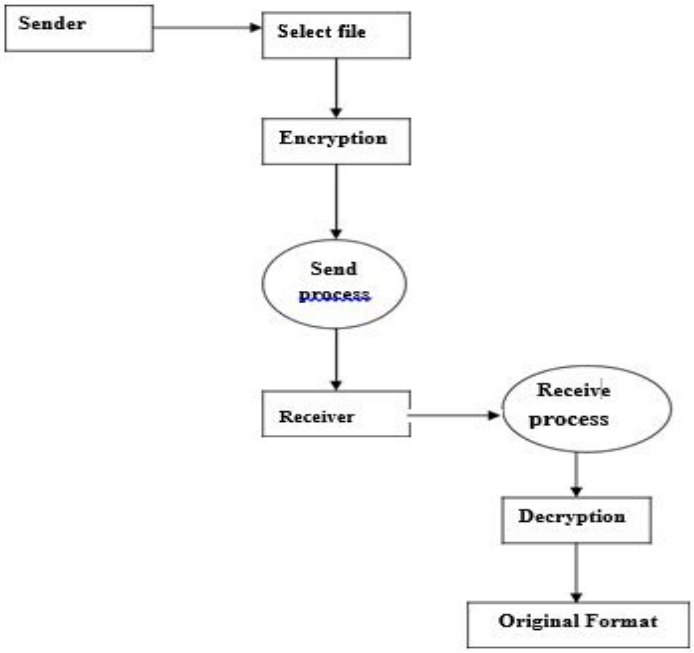


Fig. 5. Data Encryption and Decryption

VIII. ALGORITHM FOR DATA TRANSMISSIONAES ALGORITHM

On January 1997 in the US, the National Institute of Standards and Technology (NIST) announced a contest to develop an encryption system and asked for some important restrictions. The developed system had to be publicly disclosed, unclassified, free for use worldwide, usable with 128, 192 and 256 bit key sizes, and symmetric block cipher algorithms for blocks of 182 bits. On 26May 2002, 3DESwas replaced by Advanced Encryption standard (AES). AES and 3DES are commonly used block ciphers, and which one to choose depends on the requirement. AES out performs 3DES both in software and in hardware. AES is based on the Rijndael algorithm, created by Joan Daemen and Vincent Rijmen, which is a combination of a strong algorithm with a strong key. The Rijndael block cipher can use different block and key lengths, such as 128,192 and 256 bit. This versatility can produce faster and more secure symmetric block ciphers. Another algorithm which might be considered as an alternative to the Rijndael block cipher is the two fish algorithm, which can use blocks of 128 bits with keys up to 256bits. The Rijndael algorithm's combination of security, performance, efficiency, implements ability and flexibility made it an appropriate selection for AES.

IX. CONCLUSION

There are many authentication schemes in the current state. Some of them are based on user's physical and behavioural properties, and some other authentication schemes are based on user's knowledge such as textual and graphical passwords. Among the various authentication schemes, textual password and token-based schemes, or the combination of both, are commonly applied. However, as mentioned before, both authentication schemes are vulnerable to certain attacks. Moreover, there are many authentication schemes that are currently under study and they may require additional time and effort to be

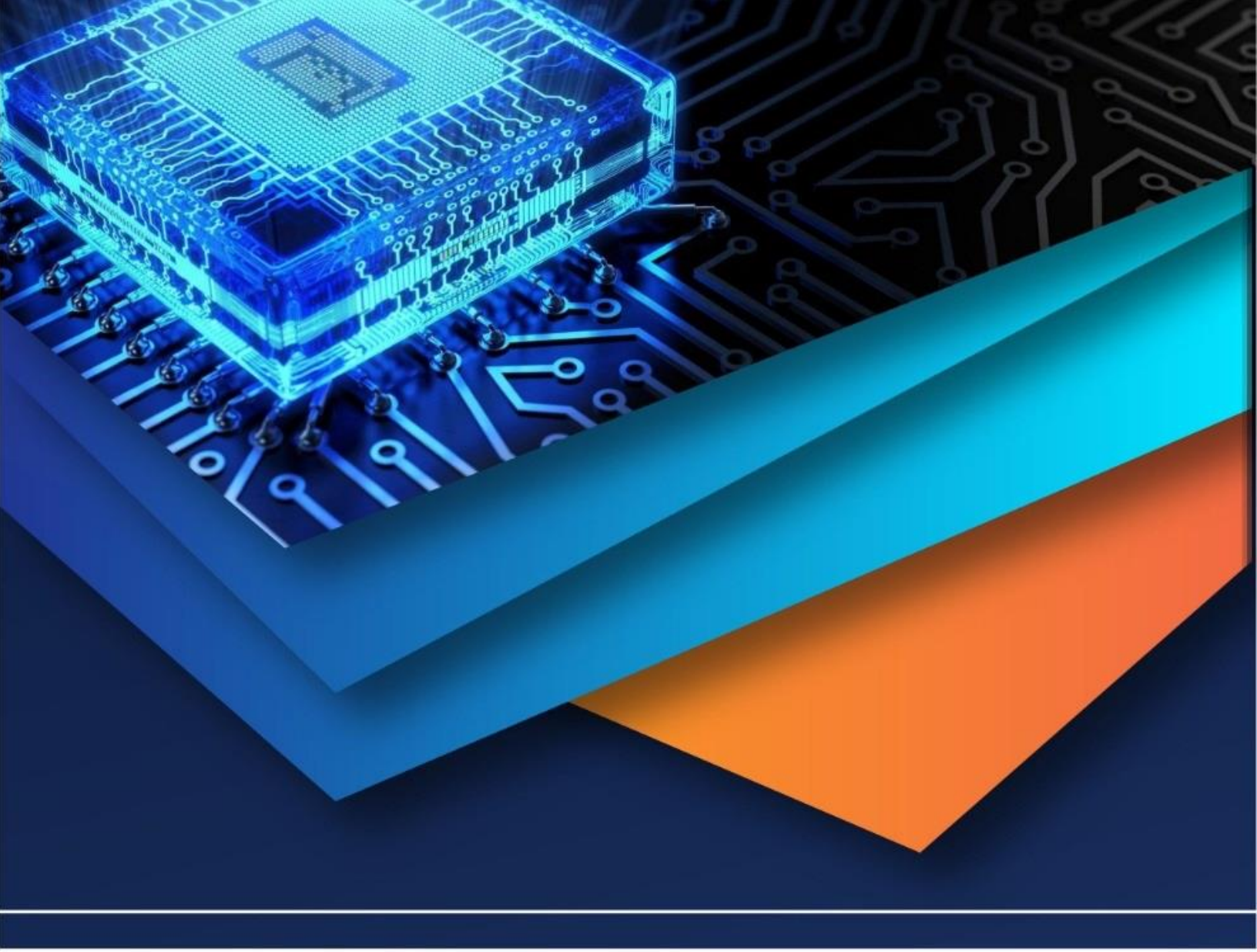
©IJRASET: All Rights are Reserved

applicable for commercial use. The Multi-dimensional password is a multifactor authentication scheme that combines these various authentication schemes into a single 3-D virtual environment. Therefore, the resulted password space becomes very large compared to any existing authentication schemes. The design of the 3-D virtual environment, the selections of objects inside the environment, and the object's type reflect the resulted password space. Additionally, designing a simple and easy to use 3-D virtual environment is a factor that leads to a higher user acceptability of a multi factor authenticated system. A user who prefers to remember and recall a password might choose textual and graphical passwords. For more security bio-metric is also used for secure transaction. This system is user friendly so everyone can use easily. Proper documentation is provided. The end user can easily understand how the whole system is implemented by going through the documentation. The system is tested, implemented and the performance is found to be satisfactory. All necessary output is generated. Thus, the project is completed successfully.

REFERENCES

[1] Multi-factor Authenticated Key Exchange
AUTHORS: David Point cheval and Sebastian Zimmer, 2008.
[2] Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards
AUTHORS: Xiao-Min Wang, Wen-Fang Zhang, Jia-Shu Zhang, Muhammad Khurram Khan, Computer Standards & Interfaces, 2007
[3] Two-factor mutual authentication based on smart cards and passwords
AUTHORS: Tianjie CAO, Shi HUANG, 2013
[4] Efficient Multi Factor Authenticated Key Exchange Scheme for Mobile Communications
AUTHORS: Rui Zhang, Yuting Xiao, Shuzhou Sunand Hui Ma, 2017
[5] Enhancing security and privacy in biometrics-based authentication systems
AUTHORS: N. K. Ratha, J. H. Connell and R. M. Bolle, IBM SYSTEMS JOURNAL, VOL 40, NO 3, 2001.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)