SMART SECURITY CONTROLS FOR STRIKERS FOR DYNAMIC COMPUTING MODELS

Ravi, N.Ch.

Associate Professor,
Dept of CSE, Pallavi Engineering College,
Hyderabad
ravi@saimail.com

Naresh Babu Muppalaneni

Assistant Professor,
Dept of CSE, NIT Silchar.
nareshmuppalaneni@gmail.com

Dr. A. Govardhan

Professor in CSE,
JNTUH CEH, T.S
govarhdhan_cse@yahoo.co.in

Joshi Padma, N.

Associate Professor,
Sreyas Institute of Engineering and Technology,
Hyderabad
padmajoshi2015@gmail.com

Abstract

Organizations are making use of Access and Identity Management systems in order to manage identity of consumers and access privileges. Such systems are acting as a significant source of identity and to fetch data. Process of protecting and safety of sensitive data from suspicious intruders and cyber assaults are useful for important tasks. A well-defined authorization process is required to ensure that appropriate people have access to appropriate data at appropriate time and with the appropriate rights. However there have been several Identity and Access mechanism to provide authentication and authorization in order to allow secure access. But previous models have their own limitations. Considering the issues of previous access model, this research work has proposed an integrated security mechanism for the safely of web application and Content delivery Networks. The authorization model is being studied in order to create safe and user-friendly web-based applications that use OTP, encryption, and the block chain concept. Several access control models, as well as their properties, have been compared to a proposed security model in research. Proposed work has used OTP to provide security during transactional operations; encryption is protecting content from being decoded by unauthentic person. The blockchain mechanism has been applied in order to secure identity. The integration of OTP, encryption and blockchain is going to play significant role in identity and access management.

Keywords: Block chain, Security, Authorization, Web Applications, Access control, OTP, Authentication**.**

1. Introduction

Proposed research has focused on the access control mechanism by making use of one time password. Research is also considering applicability of cryptography in order to secure the user password. On other hand block chain mechanism has been integrated in order to enhance the security during identity management.

1.1. *Access Control Models*

1.1.1.DAC (Discretionary Access Control)

As part of DAC paradigm, employee's access to specific application is determined by employees identify & user group to which employee belongs [10]. Active Directory user group for every appliance are common implementations of the DAC technique. Members of the AD user group may use the application. Even though this design is acceptable for application-level authorization & authentication, it is inflexible when several levels of permission are applied.

1.1.2.RBAC (Role Based Access Control)

In comparison to other forms of access management, the role-based approach is extra flexible and manageable. Access rights or application roles are used in this technique to define and regulate the level of authorization. Roles and privileges associated with each user ID are stored in application database [11]. In order to do access provisioning and user, IAM system uses database connections to role-based database. Since user's rights can't be changed in reaction to changes in the environment or business policies, this paradigm has the drawback of making it difficult to dynamically regulate the user's privileges

1.1.3.ABAC (Attribute Based Access Control)

ABAC is a highly adaptable & scalable paradigm in support of access management. Access rights for users are determined by taking into consideration user characteristics, resource characteristics, environmental conditions, and company regulations [12]. With evaluate user's authorization in support of every action in application, information must be gathered from various sources and assessed against a set of access determination criteria. This process has an impact on performance of application. Implementation of the ABAC paradigm is tough.

1.1.4.RuBAC (Rule Based Access Control)

In this access control, the control mechanism set by administrator integrates preset rules like time frame or exhibiting mobile device or keys with small hand held remote control device and checks these access credentials of user with access rules to grant or deny access.

1.1.5.MAC (Mandatory Access control)

This access control often used by government, defense organizations. This MAC standards defined by System administrator to implement strictly by security kernel and operating system to allow access to a resource objects in file system which cannot be altered by end user. This restricts individual resource owners to deny or give access to objects in file system.

1.2. *OTP*

There is always security threat to electronic commerce application. Electronic commerce allows user to buy the product online. But there is always threat from external attack. In our research we have made the transaction more secure by introducing security mechanisms. Here the concept of tradition OTP has been updated by introduction of pattern based OTP. The authentic users have to generate OTP during transaction in order to perform secure transaction. The generated OTP would be the random number. It cannot be predicted but it is generated as per users pattern based input. In this research we have made the product entry system and user sign up system along with order placement and secure transaction system.

1.3. *ENCRYPTION*

Using a cryptographic technique, data has been protected. When a message or file is encoded so that only the intended recipient can access it, it is known as encryption. An encryption key is used to unlock the information that has been scrambled, or encrypted, for the recipient. An encrypted transmission's plaintext is referred to as the "plaintext" portion of the message. Encrypted and unreadable cypher texts are known as cipher text. As simple as altering letters, encryption is possible. As encryption evolved, the process of decoding became more difficult. Wheels and gears might be used to develop more complicated encryption schemes. Computer algorithms have replaced mechanical encryption.

1.4. *BLOCK CHAIN*

While the technology behind blockchain may look complex, its underlying concept is really rather simple. To fully appreciate blockchain, one must first grasp the concept of a database. Databases are collections of electronic data stored on computer systems. To make it simpler to find particular information in a database, data is often organised in table style. Data for a single person or a small group is stored and accessed using spreadsheets. Database is built to retain far larger amounts of content and to allow many users to view, filter, and change that data simultaneously. A block chain approach has been used to establish identity management.

1.4.1. Summary

In introduction part the access control mechanism has been explained with encryption, OTP and blockchain. The literature review section is presenting the previous researches and problem statement section is presenting the limitation of existing researches. Proposed work is presenting the solution for the issues that have been faced in previous works. The result section has compared the functionality and suitability of proposed work to previous researches. Finally the conclusion part is presenting how proposed work played better than previous researches. Moreover the scope of research part is showing what could be further enhancement.

2. Literature Review

Indu et al. [1] developed a hybrid authentication and authorization paradigm for web-based applications in 2016. For the management and regulation of employee identification as well as access credentials, IAM solutions are frequently employed in businesses. IAM system provides single, reliable source of identifying & access information. For an organization's success, safeguarding and securing this sensitive information from malicious insiders & cyber attacks is essential. In order to ensure that only appropriate individuals have access to right applications at right time, enterprises require a well-defined authorization & authentication approach. Authentication and authorization may be done using variety of Identity & Access Management models; however those models have limits when it comes to implementation. For secure & easy to use web-based applications, this paper provides a hybrid authentication and authorization paradigm, which takes into consideration the disadvantages & implementation pain points of current IAM techniques. Suggested hybrid model is compared to several access control models and their properties in this article.

In 2017, Sciancalepore et.al [2] OAuth-IoT: An access control framework for the Internet of Things based on open standards. While the Internet of Things is breaking into the market, the controlled access to constrained resources still remains a blocking concern. Unfortunately, conventional solutions already accepted for both web and cloud applications cannot be directly used in this context. In fact, they generally require high computational and bandwidth capabilities (that are impossible to reach with constrained devices) and offer poor interoperability against standardized communication protocols for the Internet of Things. To solve this issue, this contribution presents a flexible authentication and authorization framework for the Internet of Things, namely OAuth-IoT. It leverages and properly harmonizes existing open-standards (including the OAuth 2.0 authorization framework, different token formats, and the protocol suite for the Internet of Things tailored by the Internet Engineering Task Force), while carefully taking into account the limited capabilities of constrained devices. Functionalities and benefits offered by OAuth-IoT are pragmatically shown by means of an experimental testbed, and further demonstrated with a very preliminary performance assessment.

Salama et al. [3] published their findings in 2017. Many aspects of our life are being transformed by the IoT. In the healthcare industry, IoT takes the shape of mobile medical applications that connect to a variety of sensors to provide healthcare practitioners with real-time information about their patients' health. However, preserving patients' privacy through an effective access control mechanism is a fundamental difficulty for IoT-based healthcare systems. An ambient house solution design that protects patients' privacy is proposed in this study. We focus primarily on two issues: 1) how to use environmental and biometric sensor data to undertake high-level activity detection tasks, and 2) how to safeguard healthcare data obtained via effective access control. To provide multi-level access control, we employ ABAC for authorisation and PKI for authentication. Our access control system controls access to healthcare content by categorising healthcare workers & content. As part of our system, we have security rules and guidelines for identifying classes & healthcare professional groups that regulate access to data. A wide range of additional policy rules, professions, and data categories may be added to the system, making it more flexible.

Researchers from Diogo Fernandes et al. [4] Security issues in cloud computing: 2014 poll Enticing features of cloud computing have spurred the industry to integrate cloud environments, which in turn has sparked academic and corporate research into related technologies in the last few decades Cloud hosting providers are taking control of on-premises infrastructures and moving them to remote data centres where they may be accessed through the

Internet and maintained by cloud hosting providers that charge on a pay-as-you-go basis. Security concerns have been raised as a result of the adoption of this new computing paradigm. Besides the problems caused by Web and Internet technologies, there are concerns with clouds that must be resolved before further cloud deployments can be made. As a result of a thorough review of the existing research on cloud security issues, this report fills in any gaps. A taxonomy is proposed for categorising many key issues, such as vulnerabilities, threats, and attacks. Additionally, it provides a complete introduction of cloud security, as well as a discussion of numerous open research topics that are currently being explored.

Tianfield H. et al., [5] Security Issues in Cloud Computing. This presentation provides a thorough examination of the security difficulties and issues in cloud computing. We begin by examining the effects of cloud computing unique properties, such as multi-tenancy, elasticity, and third-party management, on security needs. Then we look at the cloud security needs in terms of the most important concerns, such as confidentiality, integrity, availability, trust, audit, and compliance. We also go through the taxonomy for cloud computing security risks. Finally, a cloud security architecture is used to outline the security challenges in cloud computing.

Yan Yang et al. [6] published a paper in 2014. Identity and Access Management Architecture is in place in the cloud. It is required to meet cloud's security problems. This article describes that addresses a number of new issues that the cloud computing paradigm has introduced in area of it. To address some of constraints of the present architecture, the design considers the problem of security access granted by users to access cloud resources and users uploading resources. To establish a standardised and scalable design, the architecture employs security as a service technology, and the suggested specialised architecture may be applied.

Younis A. et al., [7] published a study in 2014. Cloud computing is now widely regarded as one of the most influential concepts in the IT sector. On-demand services like SaaS, IaaS, and PaaS. In spite of this, cloud computing has a number of problems, such as data security issues, cloud service abuse by malicious insiders and cyberattacks. Access control is a critical component of cloud computing security since it keeps out unauthorised users and safeguards the assets of the enterprise. Although MAC and RBAC have been used in a variety of scenarios, these models may not be able to fulfil cloud's access control needs. A broad range of users with differing security needs are involved in cloud computing. Multiple tenants and a wide variety of domains with varying security policies and procedures complicate matters further. According to the findings, conventional techniques to access control leave significant gaps in cloud computing's access control needs. A cloud access control architecture based on the findings of this research is also provided. It is our opinion that the proposed solution may not only allow for safe resource sharing across potentially untrustworthy tenants, but also support multiple access rights for the same cloud user, enabling him or her to securely utilise several services.

An article on IdM for cloud computing privacy & dynamic federation was published in 2012 by Sanchez R and colleagues [8]. Cloud computing is a logical evolution of distributed computing, SOA, and consumer electronics that has evolved over the last several decades. Security & identity management challenges have developed because of the volatility and diversity of this complex ecosystem. It is for this reason that the use of federated dynamic identity management with privacy upgrades has become a critical component of any successful adoption of Cloud technology. Our design is built on SAMLv2/ID-FF-compliant privacy and reputation enhancements to meet these requirements.

Semantics & Syntax for XML-encoded statements regarding authentication, characteristics, & authorization, as well as protocols that transport this information, are defined in this standard. errata composites are documents that include the original specification language as well as errata fixes. By design, corrections are limited to clarifying or conflicting specification wording or clarifying ambiguous. Strike-through text indicates deletions from original specification, whereas blue underlined text indicates additions. [9]

Attribute-Based Access Control Model was published by Lanjing Wang et al. [10] in 2010. As the Internet's distributed computing capabilities have increased, Web Services have become more prevalent. It's becoming more common for apps to be implemented in many environments. In spite of this, the traditional RBAC system is plagued by a number of problems, including challenges in assigning user roles and mapping data. A Web Services access control paradigm based on attributes is offered in a multi-domain situation. While RBAC's shortcomings may be remedied by using attributes that go beyond roles, this approach also provides a more dynamic, granular approach to access control. Meta-policy and Meta-attribute may be used to specify the characteristics & policies in local domains.

2010 saw the publication of Yonghe Wei et al. [11]. Attribute & role-based access control architectures are often utilised in service-oriented environments. This study proposes an attribute and role-based access control paradigm based on an examination of service access control needs. After going over each component in detail,

we've reviewed how they all fit together. Concepts of business and service roles are defined in the proposed model, as well as a mechanism for automatically creating service roles based on attribute criteria for assigning individuals to service roles. Finally, we provide a way to regulate who has access to the service. Fine-grained policy controls and service access control may be provided by this paradigm, which is independent of mechanisms.

V. C. Hu et al. [12] issued a handbook in 2014 on the concept and aspects of attribute-based access control (ABAC). Federal agencies may use ABAC described in this study. It is a logical access control system that analyses subject, requested operations and object, & in certain cases, environmental circumstances, against policies, rules that characterise allowable activities for given set of attributes. How ABAC may help firms share more information while yet maintaining control over their data is also discussed in this article.

This taxonomy of cloud identity management security challenges and solutions was released in 2014 by Umme Habiba et al. [13]. One of the most complex computer systems on the market today is a cloud-based computing platform. Today's cloud applications make use of a huge number of geographically scattered systems that are linked and used in different ways. Cloud identity management is critical to the long-term viability of any Cloud service, particularly in light of recent attention paid to the rapid spread of Cloud computing on a massive scale. A lot of attention has been dedicated to this issue by the IT industry. However, there have been a number of Cloud IDMSs on the market, although the bulk of these systems are not generally recognised or considered as very trustworthy. It is necessary to do more thorough study on Cloud-based IDMSs and their level of security in order to attain dependability and effectiveness in IDMs.

Access Control Models/ Features	**DAC**	**Entitlement/RBAC**	**ABAC**	**Proposed Hybrid Model**
De-provisioning / Provisioning	Mandatory User Group requires provisioning	Roles provisioning / Mandatory Application database requires Entitlements	Not Required Maintaining mechanism for PDP, PIP and PAP is necessary	Not Required Privileges are dynamically determined. Authorization & Authentication are through SAML2.0 technology
Reconciliation /Aggregation	Mandatory Requires to perform the aggregation from User Groups	Mandatory Requires to perform the aggregation from application database	Mandatory Requires to perform aggregation from PIP	Not Required Privileges are dynamically determined at IAM system
Access to Application Database	Not Required Only Access to active directory is required	Required User privileges are maintained in the application database	Not Required Only requires access to PDP and PIP	Not Required Application database is not used for storing any kind of user privileges
Ease of governance/certification	Required For recertification in certain intervals	Required For recertification in certain intervals	Implementation is difficult	Implementation is easy
Control over the Application Privileges	No authorization control, Only application level authentication	Organizational policies / More Difficult to apply environmental conditions	Chances affects performance of application, More Difficult to implement	Dynamically determines application privileges, Easy to implement

Table 1. Comparison of various access control models

3. Problem Statement

However there have been several researches in field of access control but still there is need to improve the protection. The previous access control systems provided limited access control features that are not sufficient to protect data from sql injection, brute force attack, man in middle attacks. The proposed research has considered the security for sql injection and several other attacks by building web-based applications where OTP, Encryption and block chain concept have been used.

4. Proposed Work

4.1.Blockchain Hybrid Approach

Process of protecting and protection of confidential data from suspicious intruders and cyber assaults are useful for essential tasks. A well-defined authentication and authorization procedure is required to guarantee that the appropriate parties have access to appropriate content at appropriate time and with the appropriate rights. However there have been some Identity and Access system that include identification and authorization in order to enable safe access. But previous versions had their own limits. Considering the problems of previous access model, this research study has suggested an optimized protection mechanism for the safely of web application. The research is looking at authentication and authorization models in order to provide robust and user-friendly web-based apps that employ OTP, encryption, and block chain definition. Research has contrasted many access control models along with their features to proposed protection model. Proposed work has used OTP to provide protection during transactional operations; encryption is preventing content from being decoded by unauthentic user. The block chain mechanism has been implemented in order to protect identities. The combination of OTP, encryption and block chain is going to play significant role in identification and access management.

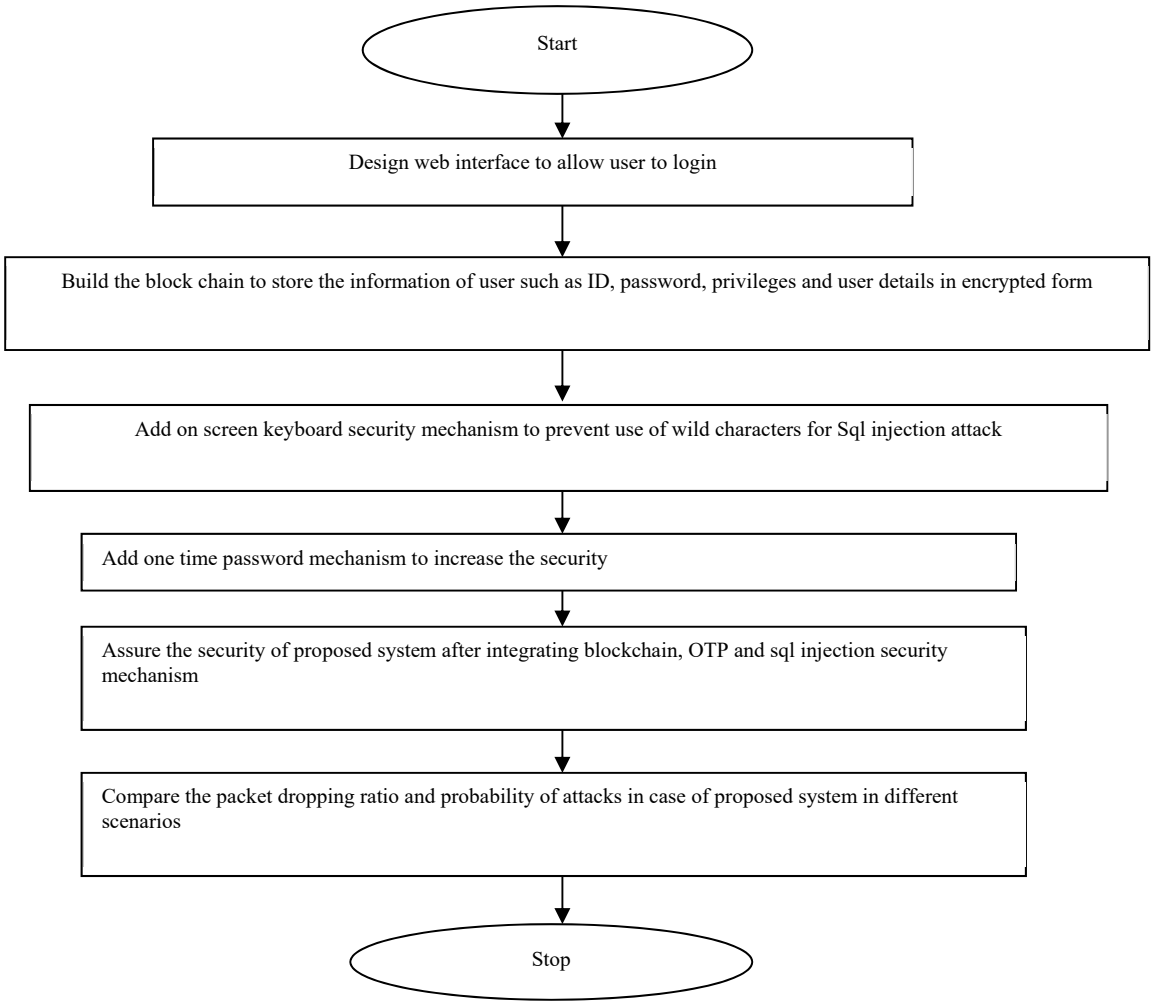

Fig.1. Process flow of proposed work

4.2.Integrated Access Control Frameworks Hybrid Approach

This block chain hybrid access control integrated with a number of other set of application frame work access controls like advanced deep learning methods with transformers of multi head attention, regular expression classifiers, tokenization, vectorization, context sensitive sanitization access controls, pattern locking, multiplicative inverse algorithms, cognitive, A.I, deep learning based firewalls etc. to detect and prevent both sql injection and Cross site scripting attacks. This will be discussed in next research work and in this we will implement only Block chain Hybrid approach.

5. Result And Discussion

The result section is presenting how the on screen keyboard has been integrated in web interface in order to restrict sql injection attack. The on screen key board is not allows user to enter the wild characters that could allow hacker to take advantage of limitations of sql queries. The use of on screen key board has enhanced the access control by restricting user to enter password that should not contain any wild character that might cause security threats to system.

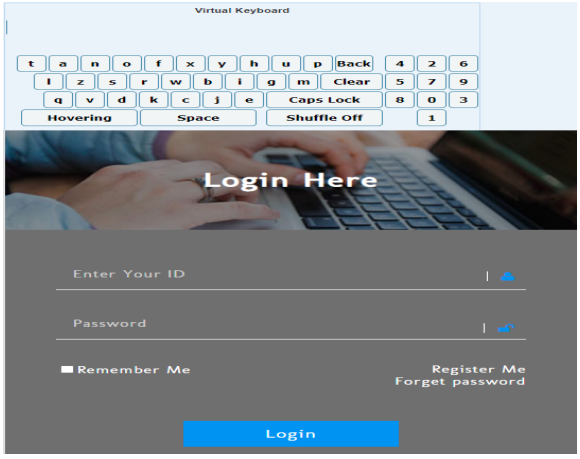

Fig.2. Onscreen keyboard on login form

In phase two the otp is generated in order to provide more security to system. This is one time password that is send to user on their email id. After getting OTP on email id user could enter it in Enter OTP form to precede login operation.

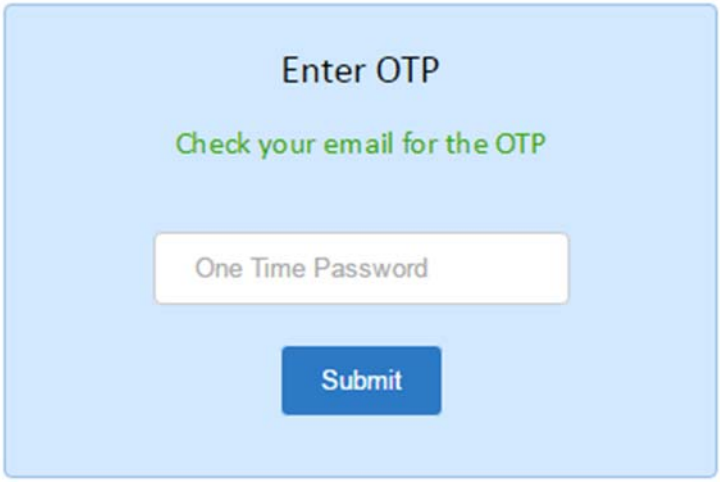

Fig.3. OTP Verification

5.1. *Role Of Blockchain In Web based User Interface*

The blockchain mechanism is working in 4 steps where user is placing request to access web application via smart contract in first step. This smart contract would send notification for sharing access to user to web application in second step. The login mechanism after check the privileges of user would accept user request and provide access during third step. Finally, in forth step the trust score gets updated at block chain.

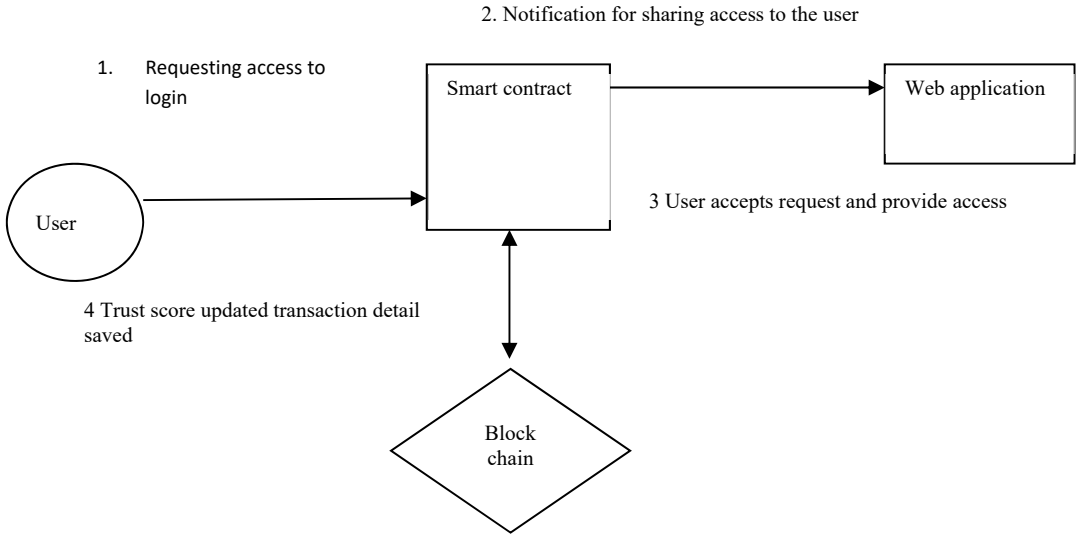

Fig. 4. Working model of block chain for access control for web application

The simulation that are presenting the probability of packet dropping in case of research that are considering only OTP, research that are making use of OTP and Sql injection prevention mechanism and the proposed research that is providing integrated solution that is making use of sql injection, OTP and block chain.

Number of packets	Packet dropping in case of OTP based security	Packet dropping in case of OTP based and Sql injection security	Packet dropping in case of Proposed hybrid approach
1000	0.1848 x 104	0.1721 x 104	0.8147 x 103
2000	0.3287 x 104	0.3091 x 104	1.8268 x 103
3000	0.5349 x 104	0.2476 x 104	0.8355 x 103
4000	0.8372 x 104	0.4490 x 104	3.8596 x 103
5000	1.1214 x 104	0.7213 x 104	4.7858 x 103
6000	0.8876 x 104	0.3382 x 104	0.8513 x 103
7000	1.6852 x 104	1.2262 x 104	5.5455 x 103
8000	1.4551 x 104	0.7079 x 104	0.2857 x 103
9000	1.9616 x 104	1.2928 x 104	6.1086 x 103
10000	1.2189 x 104	1.0477 x 104	3.9223 x 103

Table 2. Comparison chart of packet dropped

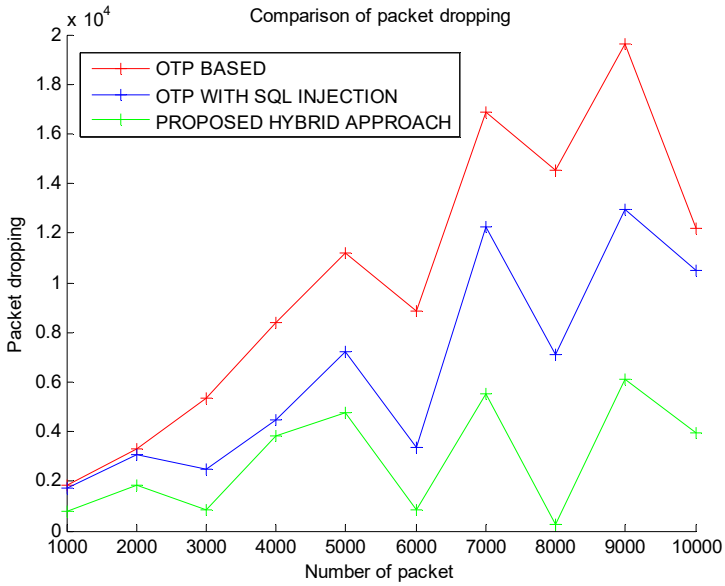

Fig. 5. Packet dropping

Number of packets	Packet affected in case of OTP based security	Packet affected in case of OTP based and Sql injection security	Packet affected in case of Proposed hybrid approach
1000	0.1512 x 104	0.1006 x 104	0.7513 x 103
2000	0.5099 x 104	0.3180 x 104	1.3982 x 103
3000	0.2505 x 104	0.2058 x 104	1.6416 x 103
4000	0.5410 x 104	0.4393 x 104	1.0300 x 103
5000	0.9935 x 104	0.5289 x 104	4.0714 x 103
6000	0.4786 x 104	0.3279 x 104	2.0999 x 103
7000	1.0087 x 104	0.7625 x 104	4.3123 x 103
8000	1.5727 x 104	1.1329 x 104	6.6466 x 103
9000	1.7642 x 104	1.0827 x 104	8.2547 x 103
10000	1.7020 x 104	1.1342 x 104	7.5373 x 103

Table 3. Comparison chart of packet affected

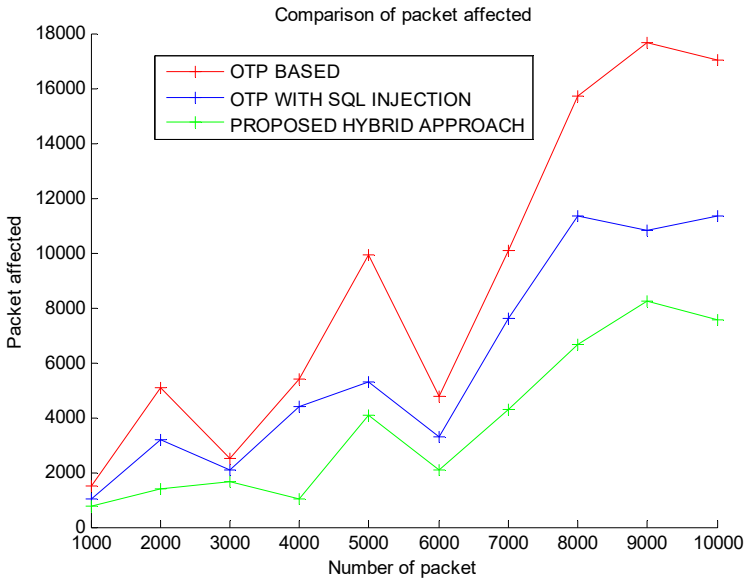

Fig 6. Packet affected

6. Conclusions

In order to keep track of an employee's identification and access credentials, firms currently deploy a wide range of identity and access management techniques. The model that has been proposed helps to overcome the shortcomings of present systems. Organizations can utilise the suggested hybrid approach to create dynamic user access control and governance policies over privileges based on user/application attributes & environmental conditions. Suggested model has a fundamental advantage over existing access control models in that it allows companies to have a safe & easy to use system to guarantee that correct people have access to the right apps with the proper credentials.

7. Scope Of Research

Making use of blockchain for user access control has enhanced the reliability and scalability of user access mechanism. Moreover the use of blockchain has provided decentralized approach. The research that are considering sql injection, man in middle attack and attack by crypto analyst end are supposed to play significant role in expanding access level security in future. This work can integrate with other set of access control frame works for detecting and preventing cross site scripting (XSS) attacks with advanced deep learning methods like transformers with multi head attention, regular expression classifiers, tokenization, vectorization, context sensitive sanitization access controls, pattern locking, multiplicative inverse algorithms, cognitive security with A.I and deep learning based firewalls etc.

References

[1] Indu, I., & Anand, P. R. (2016, March). Hybrid authentication and authorization model for web based applications. In 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) (pp. 1187-1191). IEEE.

[2] Sciancalepore, S., Piro, G., Caldarola, D., Boggia, G., & Bianchi, G. (2017, July). OAuth-IoT: An access control framework for the Internet of Things based on open standards. In 2017 IEEE Symposium on Computers and Communications (ISCC) (pp. 676-681). IEEE.
[3] Salama, U., Yao, L., Wang, X., Paik, H. Y., & Beheshti, A. (2017, June). Multi-level privacy-preserving access control as a service for personal healthcare monitoring. In 2017 IEEE International Conference on Web Services (ICWS) (pp. 878-881). IEEE.
[4] Diogo A. B. Fernandes. et. al, "Security issues in cloud environments: a survey," International Journal of Information Security, Vol. 13, Issue 2, pp.113-170, Springer, 2014.
[5] Tianfield H., "Security issues in cloud computing," Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 1082-1089, Oct. 2012, Seoul, South Korea.
[6] Yan Yang, Xingyuan Chen, Guangxia Wang, and Lifeng Cao, "An Identity and Access Management Architecture in Cloud," Proceedings of the Seventh International Symposium on Computational Intelligence and Design (ISCID), vol. 2, pp.200-203, Dec. 2014, Hangzhou, China.
[7] Younis A. Younis, Kashif Kifayat and Madjid Merabti, "An access control model for cloud computing," Journal of Information Security and Applications, vol. 19, no. 1, pp. 45– 60, Elsevier, 2014.
[8] Sanchez R., Almenares F., Arias P., Diaz-Sanchez D., and Marin A., "Enhancing privacy and dynamic federation in IdM for consumer cloud computing," IEEE Transactions on Consumer Electronics, vol. 58, no. 1, pp. 95-103, Feb. 2012.
[9] Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. [Online] https://docs.oasisopen.org/security/saml/v2.0/saml-core-2.0-os.pdf.
[10] Lanjing Wang, and Baoyi Wang, "Attribute-Based Access Control Model for Web Services in Multi-Domain Environment," Proceedings of the IEEE International Conference on Management and Service Science (MASS), pp.1- 4, 24-26 Aug. 2010, Wuhan, China.
[11] Yonghe Wei, Chunjing Shi, and Weiping Shao, "An attribute and role based access control model for service-oriented environment," Proceedings of the IEEE Control and Decision Conference (CCDC), pp.4451-4455, 26-28 May 2010, Xuzhou, China.
[12] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, "Guide to Attribute Based Access Control (ABAC) definition and considerations," NIST Special Publication, vol. 800, p. 162, 2014.
[13] Umme Habiba, Rahat Masood, Muhammad Awais Shibli, and Muaz A. Niazi, "Cloud identity management security issues & solutions: a taxonomy," Complex Adaptive Systems Modeling, vol. 2, no. 5, Springer, 2014.
[14] N. C.h. Ravi, M. Naresh Babu, R. Sridevi, V. Kamakshi Prasad, A. Govardhan and P. N. Joshi, "Inspecting Access Controls in Cloud Based Web Application," 2018 Second International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2018, pp. 262-269, doi: 10.1109/ICCMC.2018.8487896
[15] Joshi Padma, Dr.N.Ravishankar,Dr. M.B. Raju,N.Ch.SaiVyuha"Secure Software Immune receptors from Sql injection and Cross site scripting attacks in Content delivery Network Web applications" 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO 2021)DOI: 10.1109/ICRITO51393.2021,Sept. 2021
[16] Joshi Padma, Dr.N.Ravishankar, Dr. M.B. Raju, "Defensive Walls for Detecting and Preventing SQL Injection and XSS attacks in Dynamic Content Delivery Network Web Applications" Design Engineering (Toronto) ,vol.2021,issue 7,2021,pp10019-10039
[17] P. N. Joshi, N. Ravishankar, M. B. Raju and N. C.h. Ravi, "Contemplating Security of Http From SQL Injection and Cross Script," 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Coimbatore, India, 2017, pp. 1-5, doi: 10.1109/ICCIC.2017.852437
[18] P. N. Joshi, N. Ravishankar, M. B. Raju and N. C.h Ravi, "Encountering SQL Injection in Web Applications," 2018 Second International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2018, pp. 257-261, doi: 10.1109/ICCMC.2018.8487999
[19] N.CH.Ravi, Joshi Padma etal. "Advanced Access Control Mechanism For Cloud Based E-Wallet" in Volume 31 of the Lecture Notes on Data Engineering and Communications Technologies series of Springer of Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI – 2018
[20] A. Jana, P. Bordoloi and D. Maity, "Input-based Analysis Approach to Prevent SQL Injection Attacks," 2020 IEEE Region 10 Symposium (TENSYMP), Dhaka, Bangladesh, 2020, pp. 1290-1293, doi: 10.1109/TENSYMP50017.2020.9230758
[21] B. I. Mukhtar and M. A. Azer, "Evaluating the Modsecurity Web Application Firewall Against SQL Injection Attacks," 2020 15th International Conference on Computer Engineering and Systems (ICCES), Cairo, Egypt, 2020, pp. 1-6, doi: 10.1109/ICCES51560.2020.9334626
[22] A. Averin and N. Zyulyarkina, "Malicious Qr-Code Threats and Vulnerability of Blockchain," 2020 Global Smart Industry Conference (GloSIC), 2020, pp. 82-86, doi: 10.1109/GloSIC50886.2020.9267840.
[23] Joshi Padma, N. Ravishankar, M. B. Raju and N. C.h Ravi,"Surgical striking sql injection using LSTM" Indian Journal of Computer Science and Engineering ,vol.13,issue1,Feb.'2022 doi : 10.21817/indjcse/2022/v13i1/221301182 pp:208-220.

Authors Profile

Ravi, N.Ch. is Associate Professor in Computer Science and Engineering Department in Pallavi Engineering College, Nagole, Hyderabad in Telangana,India. He is also Dean R&D with 20 years experience in which 5 years in I.T Industry and 15 years in teaching. He has publications in Scopus indexed journals, Springer book chapter and IEEE. His research interest areas are Network Security, Deep learning with Transformers, Block Chain Technology and Cognitive Security. He has Logical, Programming abilities in Advanced JAVA, Spring boot, REST API, Micro services, Angular, Devops, Secure software Programming.

Dr. Naresh Babu Muppalaneni is Assistant Professor (Sr. Grade) in Computer Science and Engineering Department in National Institute of Technology, Silchar. He is Principal Investigator for 2 crores research projects of DRDO, DST completed by him. His research areas are Cryptography, Bio informatics, Computer Intelligence.

Dr. A. Govardhan is Professor in Computer Science and Engineering Department in JNTUH, Hyderabad in Telangana, India. He is also Rector of JNTUH.. He has guided 94 Ph.D theses. He has published 555 research papers at International/National Journals/Conferences including *IEEE, ACM, Springer, Elsevier, IGI Global, Taylor & Francis and InderScience*. He is an Editor for 7 Springer/ Springer Nature Proceedings. He has 3 Monographs and 10 Book Chapters in Springer

Joshi Padma N is Associate Professor in Computer Science and Engineering Department in Sreyas Institute of Engineering and Technology, Nagole, Hyderabad in Telangana, India. She worked as Head of department for CSE in Sreyas for 2.5 years. She has 19 years teaching experience and Consultant for projects in I.T industry. She has publications in Scopus indexed journals ,Springer book chapter and IEEE. Her research interest areas are Web and Network Security, Deep learning, Block Chain Technology and Cognitive Security. She has strong logical and programming skills in JAVA, Adv.Java, Spring boot, REST API, Angular and Dev ops.She did awareness Programs in Moble, Internet security in Rural areas,Villages in Schools and Colleges.