The rapid growth of credential thefts depicts the fact for urgent need to revisit the credential safety measure and embark with more user centric control. The criterion set of 11 inference rules, for protection mechanisms need to be considered while designing a new application to reduce the potential threat (T) against unauthorized access, summarized below.

1. *User Privacy (UP):* Privacy preservation is to protect the keys data and resources over the network. Sometimes a user, who tries to access data from a compromised network, does not want to reveal high-profile credentials over the network. User privacy is highly desirable for financial or business critical applications, where $T \equiv (UP)^{-1}$
2. *Privacy Preservation (PP):* A MFA should be privacy preserving for user's secrets, behavior and biometrics information should be confined only to the user. The access should consider user centric identity management. Higher the preservation lesser would be the threat i.e., $T \equiv (PP)^{-1.}$
3. *Change Flexibility (CF):* User characteristics might change; hence the MFA should be flexible enough to support these changes and application should be flexible to synchronize these changes. These flexibilities enable the greater breadth of subjects (user) to access the greater depth of objects (application) without specifying individual relationships between every subject and object. It makes access control ideal for many distributed or rapidly changing environments, hence flexibility is desirable to handle the dynamism of users and its environments. If the MFA does not support to accommodate these changes there would be larger threat with persistent user characteristics. Hence, more is this flexibility lesser is the threat i.e., $T \equiv (CF)^{-1}$
4. *Trustworthiness' (T):* A MFA is trustworthy when it considers the past behavior along with current contextual input.
5. *Relationship (R):* A MFA can consider user vs. credential relationship, which decides the permissible assignment and delegation of task. Stronger the association lesser is the relational threat.
6. *Risk Assessment (RA):* Risk assesment should include user input during insertion or setup of multifactor.
7. *Context Sensitivity (CS):* The contextual information plays a significant role in access control decisions. The MFA should be context sensitive e.g. contextual information (such as location and time) can be used to define policies for making access control decisions dynamically. Higher is this level of sensitivity(H/M/L) lesser would be the threat i.e., $T \equiv (CS)^{-1}$.
8. *User Centricity (UC):* A MFA should have extendable and richer set of user centric context (profile, capability, preference, habit, health situation). This would increase user associativity with her identities, richer is the set lesser would be the threat i.e., $T \equiv (S)^{-1}$.
9. *Adaptive Authentication (A2):* A provision of selecting the right authentication factors based on risk profiling. The decision of selecting one-factor out of two-factor or selecting few-factor out of multi-factor authentication (as per the situation e.g. risk-based authentication, presents the appropriate level of authentication for the given level of risk). It means the MFA should identify sensitive feature to provide the adaptive service. A tendency for adapting the right type of authentication is highly pertinent. Higher is the adaptability lesser would be the threat i.e., $T \equiv (A)^{-1}$.
10. *Intention Based Privilege (IP):* The application should consider user's intent. It supports sensitivity variation e.g. the high-data sensitive (HDS) activity (money transfer in banking application or password change), low-data sensitive (LDS) activity (account balance or check recent transaction). Sometimes user login to perform only LDS activity, hence ACM should be robust enough to allow LDS activity and deny HDS activity. More refined is the user requirement lesser would be the threat of exploitation i.e., $T \equiv (IP)^{-1}$. The traditional AC (one-size-fits-all authentication) methods avoids selecting only low-risk activities, while deselecting high-risk activities. However, intention-based selection can benefit financial or business critical applications. The intention-based privilege is fundamentally unaddressed in current access control Mechanisms.
11. *Granularity:* Access control mechanism should support two different types of granularity i.e. fine-grained (G^F) and the coarse-grained (G^c). Fine-grained granularity means the AC facilitate granting differential access rights to user by allowing flexibility in specifying the access rights. Coarse-grained means a collection of objects share the same AC requirements. The MFA should support a user for authorizing specific groups of objects and possibly actions. The correct mapping of fine-grained (G^F) with the coarse-grained (G^c) can allow granular control to the user for obtaining least privilege which is neither addressed in context of MFA and nor applied in access control decision. However, higher is this granularity lesser is the threat i.e., $T \equiv (G^F \& G^C)^{-1}$.

The existing MFA methods and proposed CLS framework are compared, on proposed threat reduction points discussed above and summarized in Table 1. These would help to build the user-system confidence and enhance the level of assurance.

Table 1. multifactor evluation based on inference rules

MFA Method/framework	UP	PP	CF	T	R	RA	CS	UC	A2	IP	G
1st factor of authentication Something you know	X	X	X	X	X	X	X	X	X	X	X
2nd factor of authentication Something you have	L	M	X	X	L	X	X	L	L	X	X
3rd factor of authentication Something you are	M	H	L	X	H	X	X	L	L	X	X
4th factor of authentication Someplace you are	M	X	H	L	L	X	H	X	L	X	X
CLSF	M	H	H	L	H	X	H	L	L	H	M

X- No, L-Low, M-Medium, H-High

ASSURANCE FRAMEWROK

Assurance framework chooses the most acceptable bases of the available evidence. It signifies the *"degree of trust"* graded in terms of the number of eliminated defeaters (i.e. the reasons for doubt) [19]. Initially every intruder is considered as defeaters with *"zero confidence"*. The confidence is built by eliminating the reasons of doubt on the validity of the claim (that intruder is not an attacker), evidence (of associatively) and the inference rules (for protection mechanism). As the reason for doubt are eliminated, confidence grows (eliminative induction). The concept of eliminative induction and defeasible reasoning help for developing sound and complete arguments [20], to access the select transaction of a business critical-application.

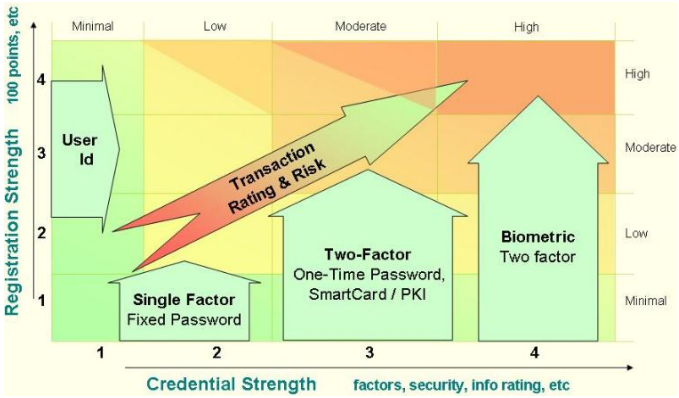

Figure 3. Credential strengthening

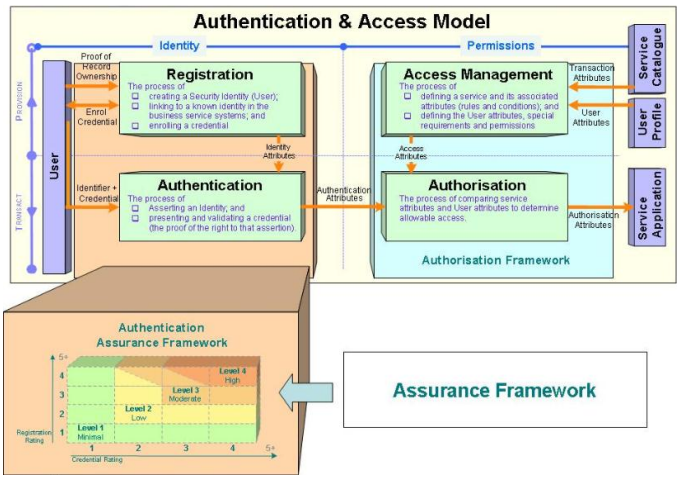

Figure 4. Assurance Framework

These arguments are based on hierarchy of expression of credentials i.e., multifactor. Our interest is to know 'how does a level of user intent strengthen the security against unauthorized accesses'. The inference rules suggest setting up the relationship among the expressions of user's intent through multifactor that should be correctly mapped with all available transactions of the system (during setup). The comfort level security CLS is a function of gradual expression of MFA for the required transaction. The user intent can consider the probable risks and request the appropriate transaction using selective expression of *MFA*. Finally, the CLS is obtained through argumentation of valid factor expressed by the end-user.

Comfort Level (CL): This notion defines the degree of security sensitivity for data and resources need to be accessed [21]. It applies the content sensitivity, i.e. the critical value of resources, data or actions e.g. consequence of changing the password. The comfort levels rates and maps with layer trust levels. The traditional monolithic access has slight detrimental effect from the confidentiality point of view. The proposed framework suggests the credential dispersal is desirable and there should be reduction of risk up to an acceptable level as illustrated in Fig. 5.

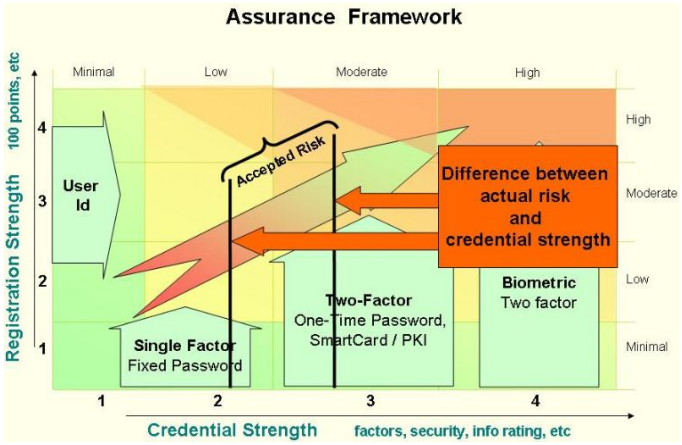

Figure 5. Assurance framework risk tolerance

CL_1S: The first level presents the minimal confidence through asserted credentials. It is used for the transaction, where an application bears minimum risk during erroneous authentication. There is no prerequisite constraint on it. However, it provides minimal assurance to its higher level that must satisfy the CL_1S authentication requirements e.g. self-registered credential or a *MAC* address satisfying a device authentication requirement, or single-factor authentication.

CL_2S: The second level of confidence is requested for transactions associated with moderate risk. Successful authentication depends on identity, proving one level above of CL_1S.

CL_3S: The third level serves a higher confidence beyond CL_2S. It is required for transactions, which might cause substantial risk during erroneous authentication. It develops higher level of trust by means of expressing multiple credentials (as factors of authentication).

CL_4S: It is required for next level for critical transactions, where erroneous authentication might cause greater hazards to the application. Hence, it demands a higher proof due to the associated risk e.g. biometric proof or tamper-resistant hardware devices (for secret or private cryptographic keys). These levels can be further enhanced. However, for low profile access, it is not mandatory to present all multifactor

and it may not always be desirable to realize the functionalities universally.

Traditional access control systems do not entertain user consideration during risk assessment and this makes them inflexible and difficult to adapt with user surroundings and circumstances [22].

FORMAL VALIDATIONOFFRAMEWORK

Mathematics is an ideal tool for modelling as it provides for high level of validation. A method is formal if it has sound mathematical basis. The present section presents the formal validation of the framework. It presents the two-factor validity, which is further generalized through induction upto *n* multifactor and proves the soundness, correctness and consistency [23] of the framework. Generalizing upto $\mathbb{R}^n$ factor authentication present attacker defender model is illustrated via game theory. We did the mathematical modelling for user and adversary in attacking steps on a business-critical application. The formal method proves how the proposed framework can reduces possibility of error, eliminates ambiguity and forms a strong theoretical basis for security assurance against unauthorized access attack.

The multifactor provides *syntactic control* which is easy to memorize and symbolize in logical semantics if it is repeated with behavioral or intentional response. Hence, introducing additional cognitive layer of safety by obfuscation.

A. Theorem 1: Soundness

Let for an individual U, 'Po' be the list of all possession vector (i.e. Biometric, Smart Card etc.). Selectively and collectively if all these factors are enrolled, all or part of it can be used during authentication phases to exhibit syntactic, semantic and cognitive constituents.

PROOF: At the *time-of-enrolment* of possession vector, a user U generates a key value m_U, which is the combination of key components, e.g. a biometric key B_m by choosing a random r_1, and/or a card-key S_m by choosing a random r_2, and so on. The combined key m should be syntactically, and semantically ordered; and resolve with cognation constituent [24]. The length and content of m_U forms the key m, makes the fresh challenge (not pre-determined). The biometric-key $B_m' = B_m$ and/or card-key $S_m' = S_m$ are expressed by the user and make the expression sound for retrievable value of m_U at the *time-of-authentication*.

B. Theorem 2 - (Two-factor Validity):

Let for an individual U, if there is a knowledge vector 'Kn' and a possession vector 'Po' (e.g. Smart Card, Biometric etc.) having its random secrets r_p or r_k. , then here is an adversary $\exists$ with either of possession or knowledge vector if the random secrets r_p or r_k is unknown to the adversary $\exists$, the framework is valid. Critical authentication will not be fully trapped until either of the secret token remains unknown to an adversary $\exists$.

PROOF: Consider the biometrics of a specific finger, that forms a knowledge vector; the swap card forms a possession vector. Let their combination forms the keym_U is generated by a user U whereas $m_\exists$is generated by an adversary $\exists$. For an individual user U, the two-factor authentication is valid with respect to the key m_U, if their enrolments are valid. The inclusion of biometric information as knowledge with possession raises entropy and makes prediction difficult due to higher random value r_ie.g., for the random secret, r_p or r_k there is high possibility that $m_\exists \neq m_U$, which makes $m_\exists$ invalid and falsifies the adversary's claim.

C. Theorem 3 - (Multi-factor Validity):

Let for an individual U, and 'Po' be the list of all possession factors (i.e. Biometric, Smart Card, Geographic location etc.) and their associated random secrets $r_1, r_2, \ldots r_n$. $\exists$ is an adversary with list of all possession factors, if the random secrets $r_1, r_2, \ldots r_n$ are unknown to $\exists$ the framework is valid. Authentication will not succeed until secret token are not in correct order and remains unknown to the adversary $\exists$.

PROOF: For an individual user U using Multi-factor authentication, let there be a contribution of user biometrics in key generation m_U while $m_\exists$is generated by an adversary $\exists$. For true m_U and valid enrolment, $m_\exists \neq m_U$ makes $m_\exists$ invalid and falsifies the adversary's claim $m_\exists$. It is difficult to do reverse engineering for biometric-key and obtain its knowledge vector. If $m_\exists$ happens to be equal to m_U the order remains unknown to the adversary and falsifies their claim. To make a genuine claim an adversary $\exists$ have to guess all random secrets $r_{i_{of\ biometric}}, r_{i_{of\ card}}, \ldots$ in correct order. It makes the task difficult for high entropies. Thus, a multi-factor authentication is valid with respect to the key generation (in an ad-hoc fashion). The key forging will reduce due to various combinations of m_U for its part's length, content and order, registered at the *time-of-enrolment*. That is also preserves the key privacy.

D. Mathematical modelling of User & Adversory

With reference to the model, underlying collection of authentication and key-distributions, we have specified an adversary $\exists$ and a legitimate user as the two players. If a legitimate user is performing all communications in the presence of an adversary. With an attack intent, the adversary tries to learn the outgoing messages along with the oracle of authentication decision (i.e. *'accepted'* or *'rejected'*). The mathematical notation of the selection vector is denoted by π^sunder a session s. The definition of *matching conversation* [25] says that an adversary is benign if deterministic and restricts its action [21].

The benign adversary $\exists$ interacts with the oracles via the query form$(i, j, s, \upsilon/\upsilon')$ i.e. sending the message υ to i, asserting it from j in a session s, interpreted as $(\pi^s_{i,j})$. Every execution can be classified as either error or !error depending on adversary's action. We evaluated CLS framework as per the secure protocol [25] defined in terms of

the distribution of conversations and decisions. The adversary can manage to subvert the run, if he/she can reach at certain decision i.e., $\delta = \{A, R, *\}$. Here $'\delta' = A/R$, suggests $'accept'$ or $'reject'$ respectively. The acceptance usually does not occur until the end of execution although rejection may occur at any time. The '*' suggests, that 'player sends no message' or 'the player has not yet reached any decision'. The υ' means 'the player presently does not have any private output'. The private output of a party will be the exchanging key (as decided by the party). The required factor avails the required level of assurance. Hence reduces the attack surface of middle arena as illustrated in Fig. 6.

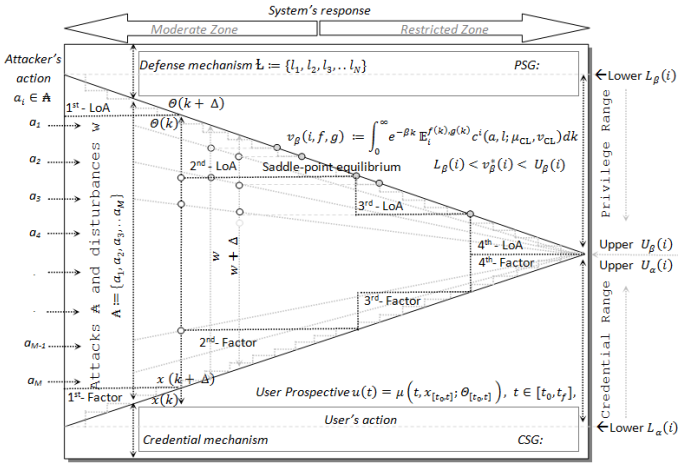

Figure 6. Attack defence mechanism fromed with MFA & Level of Assurance.

Assurance Evidence: If n is a 'Comfort Level' evidence ($n \leq m$) i.e. determined by the number of secret tokens $'ST'$, across, to which the different functionality access is dispersed, this quorum retrieves the *"functionality rights"*. The secret token $'ST'$ comprises of a randomly generated public/private key pair $priv_k/pub_k$ (locally at client side). These randomized contents of $'ST'$ need to be cryptographically strong [26]. Furthermore, n salt value $salt_i$ (alternatively, a seed to a random sequence generator stored with storage efficiency) along with its information sequence $\sigma = (n\ pw_i)$ is also stored as $'SP'$. We are not particularly leveraging on the randomness of $salt_i$ to derive security but concerned about safety. Thus, not emphasizing $'SP'$ need to be cryptographically strong.

Assurance Argument: The user and adversary $\mathcal{I}$ are the two participants request to gain access. $\sum_{i,j}(\pi^s_{a,b})$ represents the secret pattern $'SP'$[27] of selective security token $'ST'$. As per the protocol, there are two partner oracles $(\pi^s_{a',b'})$ and $(\pi^s_{b',a'})$of passive attack, where an adversary $\exists$ wants the access on the critical functionality. Hence, we need to present the supporting evidence to justify the claim. An oracle $(\pi^s_{b,a})$can break the access control security but the application can maintain the safety of high privilege operations. Execution of $(\pi^s_{a,b})$and $(\pi^s_{b,a})$ models all kinds of active attacks on $'ST'$, where an active adversary can eavesdrop all credentials between and in the $'ST'$. The pair$(\pi^s_{a,b}, m)$models the active attack, where the adversary sends $'ST'$ in$'SP'$ to get the access response. A login session can be initiated only if $m = \sigma$ matches with server oracle.

E. Mathematical modelling of Attacker & defender

The framework is crucial for business-critical application as it also forms a close system for credential vs. privilege interaction. The credentials are the multifactor and the privilege is as per the level of assurance. The interaction between attacker and defender can be captured as *zero sum*[1]and *stochastic game*[2] i.e., at an instant 't' system state Θcan be under the influence of defense action 'l' or attacker's action 'a', forming a fixed pair $(a_i, l_i), \Theta(t), t \in [t_0, t_f]$. An unanticipated event can change the system state. According to piecewise deterministic dynamics let the system state evolve from its initial known state $x(t_0) = x_0$ to $\dot{x}(t) = f(t, x, u, w; \Theta(t, a, l))$ where $x(t) \in \mathbb{R}^n, u(t) \in \mathbb{R}^r$ is the user input, $w(t) \in \mathbb{R}^p$ is the disturbance.

As per Markov jump process [28] with continuous sample paths, the rate matrix is $\lambda = \{\lambda_{ij}\}_{i,j\in S}$where $S \coloneqq \{1,2,..,s\}$is the state space and the transition rates $\lambda_{ij} \in \mathbb{R}_+$ such that for $i \neq j, \lambda_{ij} \geq 0$, and$\lambda_{ii} = 1 - \sum_{j\neq i}\lambda_{ij}fori \in S. l \in Ł$ is the cyber defense mechanism employed by the framework among all possible defense actions $Ł \coloneqq \{l_1, l_2, l_3, .. l_N\}$and $a \in \mathbb{A}$, a cyberattack chosen by the attacker among M possible action of the attack space $\mathbb{A} \coloneqq \{a_1, a_2, a_3, .. a_M\}$. The mixed strategy of defender is defined as $f(k) = [f_i(k)]_{i=1}^N \in \mathcal{F}_k$and for the attacker is defined as$g(k) = [g_i(k)]_{i=1}^M \in \mathcal{G}_k$where$f_i(k)andg_j(k)$arethe probabilities of choosing $l_i \in Ł$ and$a_i \in \mathbb{A}$, respectively. The $\mathcal{F}_k$and $\mathcal{G}_k$ are the set of admissible strategies, defined by

$$\mathcal{F}_k \coloneqq \left\{ f(k) \in [0,1]^N : \sum_{i=1}^{N} f_i(k) = 1 \right\}$$

$$\mathcal{G}_k \coloneqq \left\{ g(k) \in [0,1]^M : \sum_{j=1}^{M} g_j(k) = 1 \right\}$$

At time t, the action pair chosen by attacker and defender(a, l) forming a mixed strategy pair $(f(k), g(k))$ the transition rate or more precisely the rate matrix) is defined as.

$$\text{Prob}\{\Theta(k+\Delta) = j | \Theta(k) = i\ \lambda, a, l)\} = \begin{cases} \lambda_{ij}(f(k)), g(k)), & j \neq i, \\ \lambda_{ii}(f(k)), g(k)), & j = i \end{cases}$$

and the average transition rate is defined by

$$\lambda_{ij}(f(k)), g(k)) = \sum_{i=1}^{N} . \sum_{j=1}^{M} f_i(k) g_j(k) \bar{\lambda}_{ij}(a_i(k), l_j(k))$$

[1] One player's gain is exactly equal to the other player's loss [29].
[2]The stochastic class of model captures the micro level uncertainties and the time evolution player's strategies, by excluding the stochastic capability for transition decision; it would reduce to Markov-chain model.

The user control $u(.)$ and disturbance $w(.)$are measure able and piecewise continuous among the space denoted by U and W respectively. If (u, w) is chosen to be memoryless, it would be a Markov process [29]. On the other hand, the state informed closed loop structure has access to $x_{[t_0,t]}$ at time t for the controller and the disturbance written as.

$$u(t) = \mu\big(t, x_{[t_0,t]}; \Theta_{[t_0,t]}\big), \qquad t \in [t_0, t_f],$$

$$w(t) = v\big(t, x_{[t_0,t]}; \Theta_{[t_0,t]}\big), \qquad t \in [t_0, t_f]$$

The performance index for this hybrid control is given as $J(u, w) := \mathbb{E}_{\Theta}\{L(x, u, w; \Theta)\}$, where L is the effort for state transition $\Theta_{[t_0,t]}$, is defined as $L(x, u, w; \Theta) = q_f\left(x(t_f); \Theta(t_f)\right) + \int_{t_0}^{t_f} c\big(t, x(t), u(t), w(t)\Theta(t)\big)dt + c_0(x_0, \Theta(t_0))$,where q_f is continuous in$x$; in infinite horizon case $t_f \to \infty$ stochastic differential equation have well defined solution for each $\mu_{\mathrm{CL}} \in M_{\mathrm{CL}}andv_{\mathrm{CL}} \in N_{\mathrm{CL}}$. Markov policies provides saddle-point solution on the product space $M_{\mathrm{CL}} \times N_{\mathrm{CL}}$.

In this zero-sum two player game, the defense controller can be viewed as minimizing player and disturbance as the maximizing player [30] illustrated in Fig. 7.

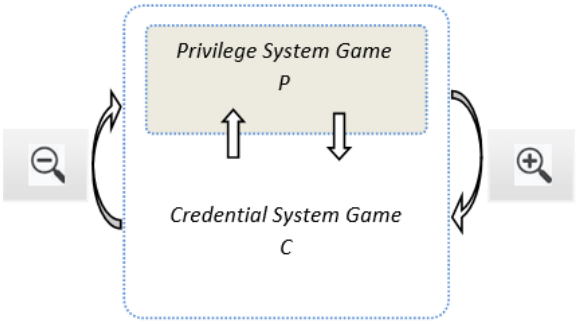

Figure 7. Privilege vs. Credential Game.

The optimal defense mechanism [31] can be imposed by applying the credential control system in return to control the privilege up to an optimal level. At a given time k the optimal privilege can be viewed by physical credential control of

$$v_{\beta}(i, f, g) := \int_0^{\infty} e^{-\beta k}\, \mathbb{E}_i^{f(k),g(k)} c^i(a, l; \mu_{\mathrm{CL}}, v_{\mathrm{CL}})dk,$$

The class of mixed stationary strategies $f^i \in \mathrm{F}^i$ and $g^i \in \mathrm{G}^i, i \in \mathrm{S}$.

$$v_{\beta}^*(i) = L_{\beta}(i) = U_{\beta}(i)$$

The incur effort $c^i(a, l; \mu_{\mathrm{CL}}, v_{\mathrm{CL}})$has two components, effort inflicted on performance index from the action pair i.e. over privilege system and impact aware credential system. The coupling between privilege mechanism and credential mechanism captures the tradeoff between resilience and security [33].

DISCUSSION AND CONCLUSION

"One size fits all" access control approach may be sufficient for non-critical application e.g., online game but the critical financial application, corporate account, group insurance etc. It may have various transactions not uniformly used however the uniform access limits the application's flexibility that would tie all the transactions and tasks to one interface. The insecurity of the multifactor would compromise of the security of the entire application, forcing various less frequently used transactions to deal with an unacceptable low level of assurance. Conversely, the proposed comfort level interface would entertain user input in the form of specific multifactor provided by the user for specific level of assurance for the intended transaction.

To reduce the potential threats against unauthorized access we discussed the 11 inference rules for protection mechanisms. While designing a new application the suggested rules can mitigate the risk of unauthorized access on various tasks by severely limiting the variety of unintended transactions. This provides an extra edge of security described with attacker defender model and formally validated with game theory. It allows application designers to relate the specific factor that best addresses user requirements for security, compatibility, and performance. The entire application can be viewed as collection of tasks of various transactions, where the selective expression of multifactor allows specific transaction stack to be built upon inter dependent tasks. We can achieve the comfort level security through proposed multifactor framework. It addresses the conflict of user intend vs. expression of credential by disallowing unintended transactions.

We argue this layered access protection mechanism can easily establish for a new design which includes complete mediation of user, separation of privilege, economical to implement, failsafe defaults and psychological acceptability. e.g., the layered architecture facilitates open design by allowing one to add another access control layer with its own security policy; this facilitates separation of privilege by disaggregating the application components and controlling the inter-AC communication.

To ensure that framework is attack proof we formally proved the two possibilities i.e., either privilege is highly restricted that no attack can cross the system boundaries or system is capable enough to recover back to its previous stable stage. In formal validation the Infinite horizon case $\mathrm{t_f} \to \infty$ states that perfect security never exists. However, the effort for perfect security limits the resource usage. The action pair yields strategic balance of privilege system for bringing back to its normal state and partial credential that prevent the framework from full failure.

REFERENCES

[1] Nakhjiri, M., & Nakhjiri, M. (2005). *AAA and network security for mobile access: radius, diameter, EAP, PKI and IP mobility.* John Wiley & Sons.ISBN-13 978-0-470-01194-2

[2] Alves-Foss, J., Taylor, C., & Oman, P. (2004, January). A multi-layered approach to security in high assurance systems. In *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on* (pp. 10-pp). IEEE

[3] Moore, S., Dimoulas, C., King, D., & Chong, S. (2014, October). SHILL: A Secure Shell Scripting Language. In *OSDI*(pp. 183-199)

[4] Chang, Y. W., Hsu, P. Y., & Shiau, W. L. (2014), 'An empirical study of managers' usage intention' in BI. Cognition, Technology & Work, 2014, 16, (2), pp. 247–258

[5] Rehman, H., Nazir, M., & Mustafa, K. (2017). Security of Web Application - State of the Art: Research Theories and Industrial Practices In: *Information, Communication and Computing Technology. ICICCT 2017*. Communications in Computer and Information Science, vol 750 (pp. 168 - 180). Springer, Singapore. https://doi.org/10.1007/978-981-10-6544-6_17

[6] Devasena, C. L. (2018). Three-Factor Authentication for Fortified Login to Ensure Privacy Preservation and Improved Security. *International Journal of Applied Engineering Research, 13*(10), 7576-7579

[7] Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Security and Privacy (SP),* 2012 IEEE Symposium (pp. 553-567).

[8] Bonneau, J. (2012). The science of guessing: analyzing an anonymized corpus of 70 million passwords. In *Security and Privacy (SP), 2012 IEEE Symposium on* (pp. 538-552). IEEE.

[9] Le, C., & Jain, R. (2009). A survey of biometrics security systems. *EEUU. Washington University in St. Louis*

[10] www.biometricgroup.com Date of access 23 Aug 2018

[11] M. Jakobsson. Modeling and Preventing Phishing Attacks. In Financial Cryptography. Springer Verlag, 2005

[12] B. Schneier. Two-Factor Authentication: Too Little, Too Late. Commun. ACM, 48(4):136, April 2005

[13] RSA White Paper. Making Sense of Man-in-the-browser Attacks: *Threat Analysis and Mitigation for Financial Institutions, 2010*. http://goo.gl/NRcez

[14] Mozilla Developer Centre. Extensions. https://developer.mozilla.org/en-US/docs

[15] S. Estehghari and Y. Desmedt (2010). Exploiting the client vulnerabilities in internet E-voting systems: hacking Helios 2.0 as an example. In *Proceedings of the 2010 international conference on Electronic voting technology/workshop on trustworthy elections, EVT/WOTE'10*, pp. 1-9

[16] S. Li, A.-R. Sadeghi, S. Heisrath, R. Schmitz, and J. Ahmad (2012). hPIN/hTAN: A Lightweight and Low-Cost e-Banking Solution against Untrusted Computers. In *Financial Cryptography and Data Security, LNCS*, pp. 235-249.

[17] VASCO. DIGIPASS GO 3, August 2012. http://goo.gl/EmLFy

[18] Adham, M., Azodi, A., Desmedt, Y., & Karaolis, I. (2013, April). How to attack two-factor authentication internet banking. In International Conference on Financial Cryptography and Data Security (pp. 322-328). Springer Berlin Heidelberg

[19] Weinstock, C. B., Howard, F. L, & Goodenough, J. B. (2007). Arguing security: creating security assurance cases. *Technical report, Software Engineering Institute, Carnegie Mellon University*

[20] Weinstock, C. B., Goodenough, J. B., & Klein, A. Z. (2013). Measuring assurance case confidence using Baconian probabilities. In *1st International Workshop on Assurance Cases for Software-Intensive Systems (ASSURE),* (pp. 7–11). IEEE

[21] Ardagna, C. A., De Capitani di Vimercati, S., Foresti, S., Paraboschi, S., & Samarati, P. (2012). Minimising disclosure of client information in credential-based interactions. *International Journal of Information Privacy, Security and Integrity 2, 1*(2-3), (pp. 205-233)

[22] Shaikh, R. A., Adi, K., Logrippo, L., & Mankovski, S. (2011, July). Risk-based decision method for access control systems. In *Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference on* (pp. 189-192). IEEE

[23] Pressman, R.,(2001). Software Engineering A Practitioner's Approach 5th Edition, ISBN 0-07-120251-X

[24] Jøsang, A., Zomai, M. A., & Suriadi, S. (2007, January). Usability and privacy in identity management architectures. In *Proceedings of the fifth Australasian symposium on ACSW frontiers-Volume 68* (pp. 143-152). Australian Computer Society, Inc.

[25] Bellare, M., & Rogaway, P. (1993). Entity authentication and key distribution. In *Annual international cryptology conference* (pp. 232-249). Springer, Berlin, Heidelberg

[26] Bernstein, D. J. (2009). Introduction to post-quantum cryptography. In *Post-quantum cryptography* (pp. 1-14). Springer, Berlin, Heidelberg

[27] Alexander, R., Hawkins, R., & Kelly, T. (2011), Security assurance cases: Motivation and the state of the art. *High Integrity Systems Engineering Department of Computer Science University of York* Deramore Lane York YO10 5GH

[28] Haidar, A., & Boukas, E. K. (2008, December). Robust stability criteria for Markovian jump singular systems with time-varying delays. In *Decision and Control, 2008. CDC 2008*. 47th IEEE Conference on (pp. 4657-4662). IEEE

[29] Zhu, Q., & Basar, T. (2015). Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems. *IEEE control systems, 35*(1), 46-65

[30] Basar, T. (2010). Lecture notes on non-cooperative game theory. *Game Theory Module of the Graduate Program in Network Mathematics*, 3-6

[31] Laszka, A., Abbas, W., Sastry, S. S., Vorobeychik, Y., & Koutsoukos, X. (2016, April). Optimal thresholds for intrusion detection systems. In *Proceedings of the Symposium and Bootcamp on the Science of Security* (pp. 72-81). ACM

[32] Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., & Cranor, L. F. (2010). Encountering stronger password requirements: user attitudes and behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 2). ACM

[33] ur Rehman, H., Khan, A. U., Nazir, M., & Mustafa, K. (2017, August). Strengthening the Defence to Cybercrimes - WannaCry Ransomware, In *3rd International Conference on Cyber Security*, (ICCS) 2017 in Kota, India.

APPENDIX - A

Authentication: It confirms the user's identity. '*who you are'* is a two-step process consisting of Identification & Authentication (I&A). Identification is how a user *'subject'* presents a specific identity (such as a username) to a system *'object'*. Authentication is the process of verifying that identity. It can be implemented by providing the username and password. This can be treated as a low-level security.

Identification and Authentication (I&A).

- Identification is the act of claiming a specific identity. Authentication is the act of verifying that identity.
- Identification uniquely identify the user (or system/ process) and shouldn't identify that user's role.

Intention: 'what you want do' defines your willingness to do specific action (transaction).

Privilege: 'what you can do in this session' defines the range of authority in a login instant.

Authorization: 'what you can do at max' defines the rights and permissions granted to a user account or process. After a system authenticated a user, authorization determines what that user can do with a system or resource.

Accountability: 'what you did' the capability to associate users and processes with their actions. Audit trails and system logs are components of accountability. Non-repudiation means that a user (username Madame X) can't deny an action because her identity is positively associated with her actions.

The Principle of Least Privilege: Assigning just the barest minimum of privilege needed for the user to perform her authorized duties.

Need-to-Know Access: The high sensitive resources are compartmentalized with implementation of additional level of formalized access approval. Subjects are granted access to these resources when they can justify their task-related reason for access.

Excessive Privilege and Creeping Privileges:

- *Excessive privilege* when a user has more access, privilege, or permission than their assigned tasks dictates. These excessive unnecessary privileges should be revoked from the user account.
- *Creeping privileges* user account accumulating privileges over the time with their job roles and assigned tasks changes. Creeping privileges result to excessive privilege. Both of these issues can be prevented with properly applying the principle of least privilege.

APPENDIX - B

Password Method

	***I**dentification **&** **A**uthentication, **Auth**orization & **Account**ability*			*Multi Factor Authentication: Something you*				*Assurance*		
Method/framework	***I&A***	***Auth***	***Account***	***Know***	***Have***	***Are***	***Behave***	***Accuracy***	***Characteristic***	***De-Merits***
Password/ Passphrase	Yes	Full	No	Yes	No	No	No	Static	Length/Static/ Limited Attempts	Complexity/Aging/ History
Kerbros	Yes	No	-	-	-	-	-	-	Dynamic	-
SSO	-	Full	-	-	No	No	No	Low	Trust based	-
OTP	Yes	Full	-	Yes	Yes	No	No	High	Dynamic	Device Dependent
S/Key protocol	-	Full	-	-	-	-	-	-	-	-
Picture Password	Yes	Full	No	Yes	No	No	No	Medium	Pictorial Memory	Low Entropy
Pico	Yes	Full		Yes	Yes	No	No	Medium	Dynamic	Device Dependent

Biometric Method

	***I**dentification **&** **A**uthentication, **Auth**orization & **Account**ability*			*Multi Factor Authentication: Something you*				*Assurance*		
Method/framework	***I&A***	***Auth***	***Account***	***Know***	***Have***	***Are***	***Behave***	***Accuracy***	***Characteristic***	***De-Merits***
Voice recognition	Yes	No	No	Yes	No	Yes	No	Medium	Analyze phonetic or linguistic patterns	text-dependent
Signature dynamics	Yes	No	No	Yes	No	No	No	Medium		
Keystroke dynamics	Yes	No	No	Yes	No	No	No	Low	Dwell, Seek/flight time producing mathematical data	Sensitivity varies w/speed & force
Iris pattern	Yes	No	No	No	No	Yes	No	High	More accurate than retina pattern & remain stable throughout life.	Lease accuracy
Retina pattern	Yes	No	No	No	No	Yes	No	Medium	Vascular pattern	Privacy concerns
Fingers/hands	Yes	No	No	No	No	Yes	No	Medium	Vascular pattern Veins pattern	Fears of eye damage

Token Method

	***I**dentification **&** **A**uthentication, **Auth**orization & **Account**ability*			*Multi Factor Authentication: Something you*				*Assurance*		
Method/framework	***I&A***	***Auth***	***Account***	***Know***	***Have***	***Are***	***Behave***	***Accuracy***	***Characteristic***	***De-Merits***
Static password	Yes	-	-	Yes	Yes	No	No	Static	Store a static password or digital certificate	Easy to crack
Dynamic password	Yes	-	-	Yes	Yes	No	No	Dynamic	Synchronous	
Challenge-response Dynamic password	Yes	-	-	Yes	Yes	No	No	-	Asynchronous	
Oauth protocol	Yes	Service	No	No	Yes	No	No	High	Partial access of API	
Open ID connect	-	Full	No	No	Yes	No	No	Low		